2600

BUSHITERA

The Hacker Quarterly

Volume 5, Number 4 Winter, 1988-89

1884 saw the beginning of public call offices.
The National Telephone Company charged 2d
(or 1p) for a three minute call.

METROPOLITAN CALLS ONLY.
AUTOMATIC BOX.

(Std. Reg. Wkg.

The National Telephone Company, Limited.

PUBLIC CALL OFFICE.

TARIFF.

LOCAL CALLS (Metropolitan Exchange Area).

For every 3 minutes conversation, or part thereof (whether originated or received), a fee of **2D.** for the use of the Call Office.

INSTRUCTIONS.

TO CALL THE EXCHANGE.—Turn the handle, place the receiver to the ear, tell operator the Exchange and number of the subscriber required, then wait with the receiver to the ear, unless the operator says she will ring you.

When requested by the operator, but not before, place two pennies in the slot and press the button after the insertion of each penny, **still keeping the receiver to your ear.** The operator has the means of checking the amount. **Bent or misshaped Pennies must not be used.**

If more than 3 minutes conversation is required the extra money must be put in at the request of the operator. Callers are only allowed 6 minutes continuous conversation.

When your conversation is finished, replace the telephone on its rest and turn the handle.

NOTES.

Unless the telephone is on its rest you cannot call or be called.

Unless the key in the handle of the telephone is kept depressed you cannot be heard by your correspondent.

When two Subscribers are connected, and one of them leaves the instrument, his telephone should be replaced on its rest, the other Subscriber keeping the receiver to his ear and replying promptly should the operator ask if he has finished.

The handle should never be turned except to call the Exchange or to get disconnected.

If Subscriber required is engaged, ask again after a short interval.

The metal passes which were some time ago issued to London Subscribers, are obsolete. Persons producing these passes will be charged the same rate as charged to a Non-subscriber.

The Clerk-in-charge of the Exchange will reply to enquiries. Operators are forbidden to converse with Subscribers.

The public are notified that their strict adherence to the above rules is absolutely essential, and that only by this can efficient working of the system be attained.

Wm. E. L. GAINE,
GENERAL MANAGER

We Know

You should have had this issue last month. We know. We're sorry.

But just because we avoided the holiday rush (by not contributing to it) doesn't mean that you'll be losing out. In fact, we used the extra time to further pursue the late breaking MCI scandal (see page 10) as well as a couple of other stories, including the latest on the famous virus.

We've been playing with our new adjunct frame (mentioned last time in this column) and are rather pleased with the results. We have all of the advantages of equal access and direct overseas dialing without having an electronic or digital switch. The extra time involved to complete a call is negligible. And touch tones are still free!

The MCI story is the first result of our new toy. As we scan out different companies and investigate them, more tales will unfold.

STAFFBOX

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Bobby Arwatt

Artwork
Tish Valter Koch

Writers: Eric Corley, Thomas Covenant, John Drake, Mr. French, The Glitch, Chester Holmes, Lex Luthor, Phantom Phreaker, Bill from RNOC, David Ruderman, Lou Scannon, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

2600 (ISSN 0749-3851) is published quarterly 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 for 1984, 1985, 1986, 1987 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 **(down at the moment)**
BBS #2 (CENTRAL OFFICE): 914-234-3260
BBS #3 (YOYODYNE): 402-564-4518
BBS #4 (BEEHIVE): 703-823-6591
BBS #5 (HACKER'S DEN): 718-358-9209
USENET ADDRESS: 2600@dasys1.UUCP
ARPANET ADDRESS: phri!dasys1!2600@nyu

A Report on the

by Bob Page
University of Lowell
Computer Science Department

(Reprinted from the RISKS Newsletter, an electronic publication available on many machines that are accessible by networks.)

***

Here's the scoop on the "Internet Worm". Actually it's not a virus -- a virus is a piece of code that adds itself to other programs, including operating systems. It cannot run independently, but rather requires that its "host" program be run to activate it. As such, it has a clear analogy to biological viruses -- those viruses are not considered live, but they invade host cells and take them over, making them produce new viruses.

A worm is a program that can run by itself and can propagate a fully working version of itself to other machines. As such, what was set loose on the Internet was clearly a worm.

This data was collected through an emergency mailing list set up by Gene Spafford at Purdue University, for administrators of major Internet sites -- some of the text is included verbatim from that list.

The basic object of the worm is to get a shell on another machine so it can reproduce further. There are three ways it attacks: sendmail, fingerd, and rsh/rexec.

The Sendmail Attack

In the sendmail attack, the worm opens a TCP connection to another machine's sendmail (the SMTP port), invokes debug mode, and sends a RCPT TO that requests its data be piped through a shell. That data, a shell script (first-stage bootstrap) creates a temporary second-stage bootstrap file called x$$,l1.c (where "$$" is the current process ID). This is a small (40-line) C program.

The first-stage bootstrap compiles this program with the local cc and executes it with arguments giving the Internet hostid/socket/password of where it just came from. The second-stage bootstrap (the compiled C program) sucks over two object files, x$$,vax.o and x$$,sun3.o from the attacking host. It has an array for 20 file names (presumably for 20 different machines), but only two (vax and sun) were compiled in to this code. It then figures out whether it's running under BSD or SunOS and links the appropriate file against the C library to produce an executable program called /usr/tmp/sh -- so it looks like the Bourne shell to anyone who looked there.

The Fingerd Attack

In the fingerd attack, it tries to infiltrate systems via a bug in fingerd, the finger daemon. Apparently this is where most of its success was (not in sendmail, as was originally reported). When fingerd is connected to, it reads its arguments from a pipe, but doesn't limit how much it reads. If it reads more than the internal 512-byte buffer allowed, it writes past the end of its stack. After the stack is a command to be executed ("/usr/ucb/finger") that actually does the work. On a VAX, the worm knew how much further from the stack it had to clobber to get to this command, which it replaced with the command "/bin/sh" (the bourne shell). So instead of the finger command being executed, a shell was started with no arguments. Since this is run in the context of the finger daemon, stdin and stdout are connected to the network socket, and all the files were sucked over just like the shell that sendmail provided.

> *"It is pretty successful in finding passwords, as most people don't choose them very well."*

The RSH/REXEC Attack

The third way it tried to get into systems was via the .rhosts and /etc/hosts.equiv files to determine "trusted" hosts where it might be able to migrate to. To use the .rhosts feature, it needed to actually get into people's accounts -- since the worm was not running as root (it was running as daemon) it had to figure out people's passwords. To do this, it went through the /etc/passwd file, trying to guess passwords. It tried combinations of: the username, the last, first, last and first, nicknames (from the GECOS field), and a list of special "popular" passwords:

aaa, academia, aerobics, airplane, albany, albatross, albert, alex, alexander, algebra, aliases, alphabet, ama, amorphous, analog, anchor, andromache, animals, answer, anthropogenic, anvils, anything, aria, ariadne, arrow, arthur, athena, atmosphere, aztecs, azure.

bacchus, bailey, banana, bananas, bandit, banks, barber, baritone, bass, bassoon, batman, beater, beauty, beethoven, beloved, benz, beowulf, berkeley, berliner, beryl, beverly, bicameral, bob, brenda, brian, bridget, broadway, bumbling, burgess.

campanile, cantor, cardinal, carmen, carolina, caroline, cascades, castle, cat, cayuga, celtics, cerulean, change, charles, charming, charon, chester, cigar, classic, clusters, coffee, coke, collins, comrades, computer, condo, cookie, cooper, cornelius, couscous, creation, creosote, cretin.

daemon, dancer, daniel, danny, dave, december, defoe, deluge, desperate, develop, dieter, digital, discovery, disney, dog, drought, duncan.

eager, easier, edges, edinburgh, edwin, edwina, egghead, eiderdown, eileen, einstein, elephant, elizabeth, ellen, emerald, engine, engineer, enterprise,

The Virus

enzyme, ersatz, establish, estate, euclid, evelyn, extension.

fairway, felicia, fender, fermat, fidelity, finite, fishers, flakes, float, flower, flowers, foolproof, football, foresight, format, forsythe, fourier, fred, friend, frighten, fun, fungible.

gabriel, gardner, garfield, gauss, george, gertrude, ginger, glacier, gnu, golfer, gorgeous, gorges, gosling, gouge, graham, gryphon, guest, guitar, gumption, guntis.

hacker, hamlet, handily, happening, harmony, harold, harvey, hebrides, heinlein, hello, help, herbert, hiawatha, hibernia, honey, horse, horus, hutchins.

imbroglio, imperial, include, ingres, inna, innocuous, irishman, isis.

japan, jessica, jester, jixian, johnny, joseph, joshua, judith, juggle, julia.

kathleen, kermit, kernel, kirkland, knight.

ladle, lambda, lamination, larkin, larry, lazarus, lebesgue, lee, leland, leroy, lewis, light, lisa, louis, lynne.

macintosh, mack, maggot, magic, malcolm, mark, markus, marty, marvin, master, maurice, mellon, merlin, mets, michael, michelle, mike, minimum, minsky, moguls, moose, morley, mozart.

nancy, napoleon, nepenthe, ness, network, newton, next, noxious, nutrition, nyquist.

oceanography, ocelot, olivetti, olivia, oracle, orca, orwell, osiris, outlaw, oxford.

pacific, painless, pakistan, pam, papers, password, patricia, penguin, peoria, percolate, persimmon, persona, pete, peter, philip, phoenix, pierre, pizza, plover, plymouth, polynomial, pondering, pork, poster, praise, precious, prelude, prince, princeton, protect, protozoa, pumpkin, puneet, puppet.

rabbit, rachmaninoff, rainbow, raindrop, raleigh, random, rascal, really, rebecca, remote, rick, ripple, robotics, rochester, rolex, romano, ronald, rosebud, rosemary, roses, ruben, rules, ruth.

sal, saxon, scamper, scheme, scott, scotty, secret, sensor, serenity, sharks, sharon, sheffield, sheldon, shiva, shivers, shuttle, signature, simon, simple, singer, single, smile, smiles, smooch, smother, snatch, snoopy, soap, socrates, sossina, sparrows, spit, spring, springer, squires, strangle, stratford, stuttgart, subway, success, summer, super, superstage, support, supported, surfer, suzanne, swearer, symmetry.

tangerine, tape, target, tarragon, taylor, telephone, temptation, thailand, tiger, toggle, tomato, topography, tortoise, toyota, trails, trivial, trombone, tubas, tuttle.

umesh, unhappy, unicorn, unknown, urchin, utility.

vasant, vertigo, vicky, village, virginia.

warren, water, weenie, whatnot, whiting, whitney, will, william, williamsburg, willie, winston, wisconsin, wizard, wombat, woodwind, wormwood.

yaco, yang, yellowstone, yosemite.

zap, zimmerman.

[I wouldn't have picked some of these as "popular" passwords, but then again, I'm not a worm writer. What do I know?]

When everything else fails, it opens /usr/dict/words and tries every word in the dictionary. It is pretty successful in finding passwords, as most people don't choose them very well. Once it gets into someone's account, it looks for a .rhosts file and does an "rsh" and/or "rexec" to another host, sucks over the necessary files into /usr/tmp and runs /usr/tmp/sh to start all over again.

Between these three methods of attack (sendmail, fingerd, .rhosts), it was able to spread very quickly.

The Worm Itself

The "sh" program is the actual worm. When it starts up it clobbers its argv array so a "ps" will not show its name. It opens all its necessary files, then unlinks (deletes) them so they can't be found (since it has them open, however, it can still access the contents). It then tries to infect as many other hosts as possible -- when it successfully connects to one host, it forks a child to continue the infection while the parent keeps on trying new hosts.

One of the things it does before it attacks a host is connect to the telnet port and immediately close it. Thus, "telnetd: ttloop: peer died" in /usr/adm/messages means the worm attempted an attack.

The worm's role in life is to reproduce -- nothing more. To do that it needs to find other hosts. It does a "netstat -r -n" to find local routes to other hosts & networks, looks in /etc/hosts, and uses the yellow pages distributed hosts file if it's available. Any time it finds a host, it tries to infect it through one of the three above methods. Once it finds a local network (like 129.63.nn.nn for ulowell) it sequentially tries every address in that range.

If the system crashes or is rebooted, most system boot procedures clear /tmp and /usr/tmp as a matter of course, erasing any evidence. However, sendmail log files show mail coming in from user /dev/null for user /bin/sed, which is a tipoff that the worm entered.

Each time the worm is started, there is a 1/15 chance (it calls random()) that it sends a single byte to ernie.berkeley.edu on some magic port, apparently to act as some kind of monitoring mechanism.

The Crackdown

Three main 'swat' teams from Berkeley, MIT, and Purdue found copies of the VAX code (the .o files had all the symbols intact with somewhat meaningful names) and disassembled it into about 3000 lines of C. The BSD development team poked fun at the code, even going so far to point out bugs in the code and supplying source patches for it! They have not released the actual source code, however, and refuse to do so. That could change -- there are a number of people who want to see the code.

Portions of the code appear incomplete, as if the program development was not yet finished. For example, it knows the offset needed to break the BSD fingerd, but doesn't know the correct offset for Sun's fingerd (which causes it to dump core); it also doesn't erase its tracks as cleverly as it might; and so on.

The worm uses a variable called "pleasequit" but doesn't correctly initialize it, so some folks added a module called _worm.o to the C library, which is produced from: int pleasequit = -1; the fact that this value is set to -1 will cause it to exit after one iteration.

The close scrutiny of the code also turned up comments on the programmer's style. Verbatim from someone at MIT: "From disassembling the code, it looks like the programmer is really anally retentive about checking return codes, and, in addition, prefers to use array indexing instead of pointers to walk through arrays."

Anyone who looks at the binary will not see any embedded strings - they are XOR'ed with 81 (hex). That's how the shell commands are imbedded. The "obvious" passwords are stored with their high bit set.

Although it spreads very fast, it is somewhat slowed down by the fact that it drives the load average up on the machine -- this is due to all the encryptions going on, and the large number of incoming worms from other machines.

[Initially, the fastest defense against the worm is to create a directory called /usr/tmp/sh. The script that creates /usr/tmp/sh from one of the .o files checks to see if /usr/tmp/sh exists, but not to see if it's a directory. This fix is known as "the condom".]

Now What?

None of the ULowell machines were hit by the worm. When BBN staffers found their systems infected, they cut themselves off from all other hosts. Since our connection to the Internet is through BBN, we were cut off as well. Before we were cut off, I received mail about the sendmail problem and installed a patch to disable the feature the worm uses to get in through sendmail. I had made local modifications to fingerd which changed the offsets, so any attempt to scribble over the stack would probably have ended up in a core dump.

Most Internet systems running 4.3BSD or SunOS have installed

Computer Networks

the necessary patches to close the holes and have rejoined the Internet. As you would expect, there is a renewed interest in system/network security, finding and plugging holes, and speculation over what will happen to the worm's creator.

If you haven't read or watched the news, various log files have named the responsible person as Robert Morris Jr., a 23-year old doctoral student at Cornell. His father is head of the National Computer Security Center, the NSA's public effort in computer security, and has lectured widely on security aspects of UNIX.

Associates of the student claim the worm was a "mistake" -- that he intended to unleash it but it was not supposed to move so quickly or spread so much. His goal (from what I understand) was to have a program "live" within the Internet. If the reports that he intended it to spread slowly are true, then it's possible that the bytes sent to ernie.berkeley.edu were intended to monitor the spread of the worm. Some news reports mentioned that he panicked when, via some "monitoring mechanism" he saw how fast it had propagated.

A source inside DEC reports that although the worm didn't make much progress there, it was sighted on several machines that wouldn't be on its normal propagation path, i.e. not gateways and not on the same subnet. These machines are not reachable from the outside. Morris was a summer intern at DEC in '87. He might have included names or addresses he remembered as targets for infesting hidden internal networks. Most of the DEC machines in question belong to the group he worked in.

The final word has not been written -- I don't think the FBI has even met with this guy yet. It will be interesting to see what happens.

MCI: The Phone Company With

It all started with what sounded like a friendly phone call in October:

"Hello, this is Patricia from MCI. We noticed that you presently have an account with MCI and we wanted to let you know that we'll be offering 'one plus' service in your area starting December 10th. We'd like to verify your address."

The nice lady then read us our address, which was one hundred percent correct. She then said another person would call us to confirm this information. That call came within minutes and was almost identical in content.

A couple of weeks later we got another one of those calls on another of our lines that had an MCI account attached to it. But this time the second call never came.

In early December, equal access came to our phone lines. We decided to check the status of those two lines that had gotten the calls. We dialed 1-700-555-4141. And guess what? They had both been claimed by MCI. Surprised? We weren't. In fact, when those calls come in, we *expected* them to try and pull this scam we'd heard so much about. They made one big mistake though -- they tried it on us.

We always listen very carefully when phone companies call us. And we can say very definitely that MCI never asked us if we wanted to choose them as our long distance carrier. All they asked us to do was to verify our address.

OK, so it was a sloppy representative. Maybe even a corrupt one. How can you condemn an entire company because of the actions of one person? That's quite easy. It happened more than once. Different representatives called different phone numbers and gave the same little speech. And we've found out that other people have gotten the same treatment. This indicates to us that these representatives are reading a script that tells them *not* to ask the customer whether they actually *want* MCI's "one plus" service. Address verification, after all, is a much less controversial issue.

Perhaps MCI feels they're taking a calculated risk here. They only seem to make these calls to people who already use MCI in some form. Maybe they feel these people won't raise a fuss when they discover who their long distance company is. In fact, they may never even discover that MCI is their carrier since they most likely have been getting MCI bills in the past. Remember, these are people who have already been using MCI's services.

Regardless of whether or not it pays off, it's distressing to see such dishonest tactics on the part of a major company.

This isn't our only gripe with MCI. We had been using an account on MCI's 950-1986 dialup. In November we paid the bill a few days late (it was under $10). Well, lo and behold, they disconnected our code without *any* warning. When we asked them to reconnect it, they said they would have to handle our payment for 10 days first. Ten days went by and the code was still down. We asked again. This time, they said they were phasing out that service, so they couldn't reconnect us. But they came up with a bright idea. We could use our 14-digit MCI Card code instead of our old 5-digit code. "It's just as easy to remember," they said.

Clearly, they have the right to phase out their services and replace them with less desirable ones. But once again, it's the way in which they did it. MCI jumped at the first opportunity to take away our old code instead of being up front and letting their customers know that as of a certain date this service would be terminated. Being sneaky about it doesn't do anyone any good.

The Real Scam

We've saved the best for last. When we discovered that MCI had selected themselves as our long distance carriers, we decided to experiment a little. One of our experiments involved trying to make an operator assisted call ("zero plus") on an MCI line. MCI doesn't offer operator assisted services. So we were curious as to

A Lot of Explaining To Do

what would happen when we tried to do this.

What happened was a big surprise. We got the same little fading dial tone that we got on AT&T -- in other words, the prompt to enter our AT&T calling card number. We entered the card number and were astounded to hear a recording say, "Thank you for using NTS."

NTS? Who the hell were *they?!* And what were they doing accepting AT&T calling card numbers on MCI lines?

We'll skip all of the drama and simply tell you what we found out. NTS is an Alternate Operator Service (AOS) company. They handle calls from hotel rooms and privately owned payphones. Their rates are often double those of AT&T. And it seems that in various parts of the country, MCI has a clandestine relationship with these people. We say clandestine because we're in the habit of reading all of the literature from every phone company that serves our area. And nowhere has this little "service" been mentioned. We have yet to find anyone in MCI who is even aware of this arrangement. On the other hand, NTS (based in Rockville, Maryland) is quite proud of the MCI connection. All of the NTS operators (who can trick anyone into believing they're really from AT&T) are aware that they provide service for MCI "zero plus" customers.

Why does MCI use an AOS? We can't imagine. But we can tell you the effects. If you decide to call someone collect from your phone and MCI happens to be your long distance carrier, the person who accepts on the other end will wind up with one hell of a surprise when they get the bill. You'll be the one getting the surprise if you forget that MCI doesn't have operators and you attempt to place an operator-assisted or calling card call through them. The most likely scenario, though, would be something like this: you visit a friend and need to make a phone call from his house. Since you don't want to make your friend pay, you dial it "zero plus" and bill it to your calling card. How are you to know that your friend selected MCI as his long distance carrier and that you've just been swindled by an AOS? Perhaps MCI's new slogan can be: "We bring the thrill of hotel phones right into your own home!"

Now we should point out that this "NTS Connection" doesn't work everywhere. In some areas you get recordings when you try to make "zero plus" calls using MCI. We need to know where it does work. You can find out at no charge by dialing 10222-0 followed by a ten digit phone number (you can use your own). If you hear a fading dial tone, it means you're about to be connected to NTS. You can stay on and ask a whole lot of questions if you want. Let us know if it works in your area. (You can do the above even if MCI isn't your primary carrier -- the 10222 routes the call to MCI. You must have equal access in your area in order to try this.)

There's really not much more to add. We are demanding a public statement from MCI addressing the issues of signing up unsuspecting consumers and billing their own customers exorbitant rates for operator-assisted calls without telling them. We don't expect to ever get such a statement.

Several years ago, we printed a story about MCI's electronic mail system, MCI Mail, which had a policy of terminating accounts that had received mail not to MCI's liking. We called it a flagrant invasion of privacy to peruse the mail of their own paying subscribers. The president of MCI indicated that he couldn't care less.

So all we can say right now is that it would be a very good idea to **boycott MCI** for all of the above reasons. A company that resorts to such devious methods of making money and that treats its customers so shabbily is not worthy of the historical significance its founders achieved.

We would appreciate it if this article was spread around in whatever ways possible.

A HACKER'S GUIDE

by Red Knight
Phreakers/Hackers Underground Network

Brief History of UNIX

It's because of Ken Tompson that today we're able to hack UNIX. He used to work for Bell Labs in the 60's. Tompson started out using the MULTICS OS. It was later eliminated and Tompson was left without an operating system to work with. He had to come up with something really quick. He did some research and in 1969 UNIX came into being. It was a single user system and it didn't have many capabilities. In a combined effort with others he rewrote the version in C and added some good features. This version came out in 1973 and was made available to the public. This was the beginning of UNIX as it's presently known. The more refined version of UNIX is known as UNIX system V. It was developed by Berkeley University and it has unique capabilities.

Various types of UNIXes are CPIX, Berkeley Ver 4.1, Berkeley 4.2, FOS, Genix, HP-UX, IS/I, OSx, PC-IX, PERPOS, Sys3, Ultrix, Zeus, Xenix, UNITY, VENIX, UTS, Unisys, Uniplus+, UNOS, Idris, QNIX, Coherent, Cromix, System III, System 7, sixth edition.

Hacking UNIX

I believe that hacking into any computer requires knowledge of the operating system itself. Basically what I will try to do is get you to be more familiar with UNIX operation and its useful commands.

Error Messages (UNIX system V)

Login incorrect - an invalid ID and/or password was entered. This means very little. In UNIX there is no way of guessing valid user ID's. You may come across this one when trying to get in.

No more logins - will happen when the system won't accept any more logins. This could mean the system is going down.

Unknown ID - will happen if an invalid ID is entered using the (su) command.

Your password has expired - This is quite rare. Reading the etc/passwd will show you at what intervals it changes.

You may not change the password - The password has not yet aged enough. The administrator sets the quotas for the users.

Unknown group [group's name] - occurs when chgrp is executed and the group doesn't exist.

Sorry - indicates that you have typed in an invalid super user password (execution of the su).

Permission denied! - indicates you must be the owner or a super user to change the password.

Sorry [# of weeks] since last change - this will happen when the password has not aged enough and you try to change it.

[directory name]: no permission - you are trying to remove a directory for which you have no permission.

[file name] not removed - trying to delete a file owned by another user that you don't have write permission for.

[dirname] not removed - ownership of the dir that you're trying to delete is not yours.

[dirname] not empty - the directory contains files so you must delete the files before executing the rmdir.

[command] not found - you have entered an invalid command which is not known to UNIX.

can't execute pwd - something's wrong with the system and it can't execute the pwd command.

TO UNIX

cannot chdir to .. - (.. means one level up) permission is required to execute pwd above the current directory.
can't open [file name] - you defined the wrong path or file name or you have no read permission.
cp: [file name] and [file name] are identical - self-explanatory.
cannot locate parent directory - occurs when using mv.
[file name] not found - file which you're trying to move doesn't exist.
You have mail - self-explanatory.

Error Messages (Basic Networking Utility)

cu: not found - networking not installed.
login failed - invalid ID or password or wrong number specified.
dial failed - the system never answered due to a wrong number.
uucp completely failed - did not specify file after -s.
wrong time to call - you called at a time not specified in the systems file.
system not in systems - you called a remote not in the systems file.

UNIX Logon Format

The first thing you must do is switch to lower case.

Here is what you will see (sometimes there will be no system identifier).

AT&T UNIX Sys VR3.0 (example of a system identifier)

login:
or
Login:

Any of these is a UNIX. This is where you will have to guess at a valid user ID. Here are some that I have come across: glr, glt, radgo, rml, chester, cat, lom, cora, hlto, hwill, edcasey, and also some containing numbers: smith1, mitu6, and some containing special characters like bremer$, j#fox. Login names have to be 3 to 8 characters in length, lowercase, and must start with a letter. In some XENIX systems one may login as "guest".

User Level Accounts

In UNIX they have what are called accounts. These accounts can be used at the "login:" prompt. Here is a list:

sys
bin
trouble
daemon
uucp
nuucp
rje
lp
adm
listen - if starlan is installed

"Super user accounts make UNIX worth hacking."

Super User Accounts

And then there are super user accounts which make UNIX worth hacking. These accounts are used for a specific job. In large systems they are assigned to users who have a responsibility to maintain subsystems. They are as follows (all lower case):
root - this is a must. The system comes configured with it. It has no restrictions. It has power over every

HACKING AWAY

other account.
unmountsys - unmounts files.
setup - system setup.
makefsys - makes a new file.
sysadm - allows useful commands (doesn't need root login).
powerdown - powering system down.
mountfsys - mounts files.
checkfsys - checks files.

These accounts will definitely have passwords assigned to them. These accounts are also commands used by the system administrator. Here are some examples of accounts I have seen:

```
   cron
   uuhelp
   usenet
   anonuccp
   news
   network
   bellboy
   lp
   vector
   guest
   games
   ninja
   vote
   warble
   sysinfo
```

Password Entry

After the login prompt you will receive a password prompt:

```
password:
   or
Password:
```

Enter the password (it won't echo). The password rule is as follows: each password has to contain at least six characters. The maximum is eight. Two of these have to be letters and at least one has to be a number or a special character.

The letters can be in upper case or lower case. Here are some of the passwords that I have seen: Ansuya1, PLATOON6, uFo/78, ShAsHi.., Div417co.

The passwords for the super user accounts will be difficult to hack. You can try the accounts interchangeably (example: login:sysadm password: makefsys). It really could be anything. The user passwords are changed by an aging process at successive intervals. The users are forced to change it. The super user will pick a password that won't need changing for a long period of time.

You Have Made It!

The hard part is over and hopefully you have hacked a super-user account. The next thing you'll probably see is the system news:

```
login:john
password:hacker1
System news
There will be no networking offered
to the users till August 15, due to
hardware problems.

$
```

$ is the UNIX prompt which means that UNIX is waiting for a command to be entered. I will use this throughout the article to show outputs, etc. (it's not a part of the command). # means you're logged in as root (very good).

How UNIX is Made Up

UNIX is made up of three components: the shell, the kernal, and the file system.

The Shell

The shell is a high level language. It has two important uses. It acts as a command interpreter. For instance, when using commands like cat, who,

ON UNIX

ls, etc., the shell is at work figuring out whether you have entered a command correctly or not. The second most important reason for the shell is its ability to be used as programming language. Suppose you're performing some tasks repeatedly over and over again. You can program the sheli to do this for you.

The Kernal

You could say that the kernal is the heart of the UNIX operating system. The kernal is a low level language lower than the shell which maintains processes. The kernal handles memory usage, maintains the file system, the software, and hardware devices.

The File System

The file system in UNIX is divided into three categories: directories, ordinary files, and special files. (d,-)

SEE FIGURE A.

/unix - is the kernal

/etc - contains system administrator's files. Most are not available to the regular user (this directory contains the /passwd file).

Here are some files under the /etc directory:

/etc/passwd
/etc/utmp
/etc/adm/sulog
/etc/motd
/etc/group
/etc/conf
/etc/profile

/dev - contains files for physical devices such as the printer and the disk drives.

/tmp - temporary file directory.

/lib - directory that contains programs for high level languages.

/usr - this directory contains directories for each user on the system.

Example of a list of files under /usr:

/usr/tmp
/usr/lib
/usr/docs

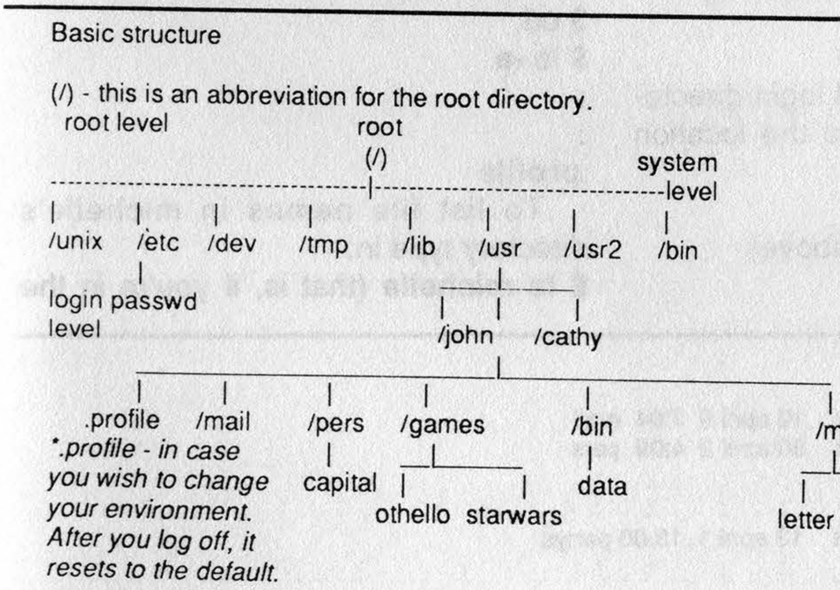


FIGURE A

/usr/news
/usr/spool
/usr/spool/lp
/usr/lib/uucp

/bin - contains executable programs (commands)

The root also contains:
/bck - used to mount a backup file system.
/install - used to install and remove utilities.
/lost+found - this is where all the removed files go. This dir is used by fsck (1M).
/save - a utility used to save data.
/mnt - used for temporary mounting.

Local Commands Explained in Detail

At the UNIX prompt, type the pwd command. It will show you the current working directory you are in.

$ pwd
/usr/admin - assuming that you have hacked into a super user account.
$

This gives you the full login directory. The / before tells you the location of the root directory.

or
(refer to the diagram above)

$ pwd
/usr/john - assuming that you have hacked into John's account.
$

Now let's say you wanted to move down to the michelle directory (you own this) which contains letters. You would type in:

$ cd michelle
or
$ cd usr/john/michelle
$ pwd
/usr/john/michelle
$

To go back one directory, type in:

$ cd ..

or to go back to your parent directory, just type in "cd".

To list file directories, assuming you are in the parent directory:

$ ls /usr/john
mail
pers
games
bin
michelle

This won't give you the .profile file. To view it type:

$ cd
$ ls -a
:
:
.profile

To list file names in michelle's directory type in:

$ ls michelle (that is, if you're in the

```
$ ls -l
total 60
-rwxr-x---   5 john    bluebox   10 april 9   7:04  mail
drwx------   7 john    bluebox   30 april 2   4:09  pers
   :           :         :          :    :      :     :
   :           :         :          :    :      :     :
-rwxr-x---   6 cathy   bluebox   13 april 1  13:00  partys
   :           :         :          :    :      :     :
$
```

FIGURE B

TO UNIX

"john" directory)

```
$ ls /usr/john/michelle
```

(parent directory)

ls -l

The ls -l is an an important command in UNIX. This command displays the whole directory in long format. Run this in the parent directory.

SEE FIGURE B.

The total 60 tells you the amount of disk space used in a directory. The -rwxr-x--- is read in triples of three. The first character (-,d,b,c) means the following: - is an ordinary file, d is a directory, b is a block file, c is a character file.

The r stands for read permission, w for write permission, x for execute. The first column is read in three triples as stated above. The first group of three (in -rwxr-x---) after the "-" specifies the permission for the owner of the file, the second triple is for the groups (the fourth column), and the last triple indicates the permissions for all other users. Therefore the -rwxr-x--- is read as follows: the owner john has permission to read, write, and execute anything in the bin directory but the group has no write permission to it and the rest of the users have no permission at all. The format of one of the lines in the above output is as follows:

file type/permissions, links, user's name, group, bytes taken, date, time when last renewed, directory or file name.

chmod

The chmod command changes permission of a directory or a file. Format is chmod who(+, -, =)(r, w, x). The who is substituted by u-user, g-group, o-other users, a-all. The + means add permission, - means remove permission, = means assign. Example: if you wanted all other users to read the file named mail, you would type:

```
$ chmod o+r mail
```

cat

Now suppose you wanted to read the file letter. There are two ways of doing this. First, go to the michelle directory. Then type in:

```
$ cat letter
line one ...\
line two ...the output of letter
line three../
$
```

or if you are in the parent directory, type in:

```
$ cat /usr/john/michelle/letter
```

and you will have the same output. Some cat options are: -s, -u, -v, -e, -t.

Special Characters in UNIX

***** - matches any number of single characters. (Example: ls john* will list all files that begin with john.)

[...] - matches any one of the characters in the [ ].

? - matches any single character.

& - runs a process in the background leaving your terminal free.

$ - values used for variables also $n - null argument.

> - redirects output.

< - redirects input to come from a file.

>> - redirects command to be added to the end of a file.

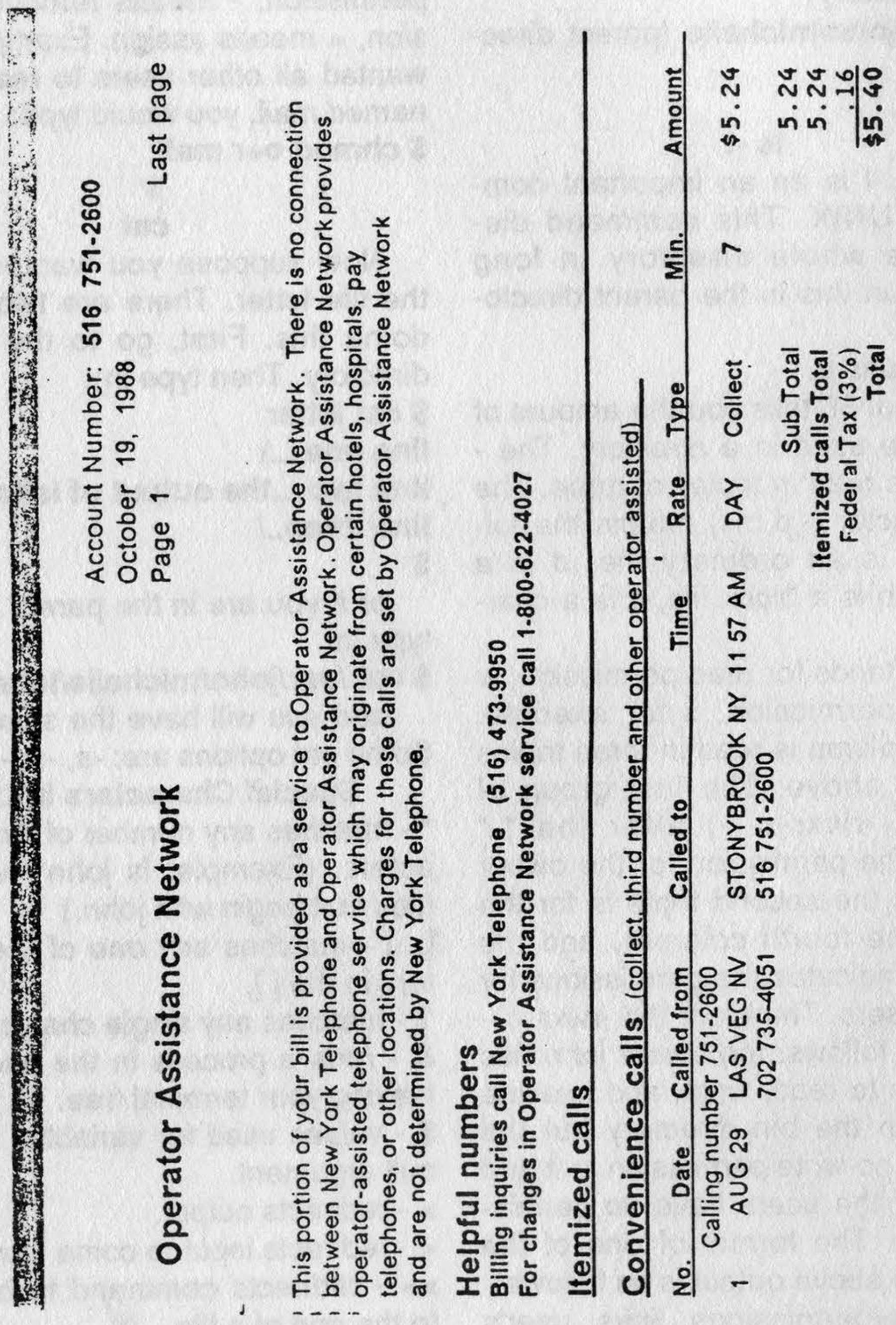
| - pipe output (Example: who|wc-l tells us how many users are online).

passwd

Password changing seems to be a big thing among some. To change the password, one would use the "pass-

(continued on page 40)

GALL DEPT.



Operator Assistance Network

Account Number: 516 751-2600
October 19, 1988
Page 1
Last page

This portion of your bill is provided as a service to Operator Assistance Network. There is no connection between New York Telephone and Operator Assistance Network. Operator Assistance Network provides operator-assisted telephone service which may originate from certain hotels, hospitals, pay telephones, or other locations. Charges for these calls are set by Operator Assistance Network and are not determined by New York Telephone.

Helpful numbers

Billing inquiries call New York Telephone (516) 473-9950
For changes in Operator Assistance Network service call 1-800-622-4027

Itemized calls

Convenience calls (collect, third number and other operator assisted)

No.	Date	Called from	Called to	Time	Rate	Type	Min.	Amount
	Calling number 751-2600							
1	AUG 29	LAS VEG NV 702 735-4051	STONYBROOK NY 516 751-2600	11 57 AM	DAY	Collect	7	$5.24
						Sub Total		5.24
						Itemized calls Total		5.24
						Federal Tax (3%)		.16
						Total		**$5.40**

IT TOOK A LOT OF GALL for someone to call us collect and somehow convince an untrained operator that we had accepted the charges and then apparently talk to our answering machine for seven minutes. It also takes a lot of gall for an Alternate Operator Service company like the above to charge the astronomical rates they do, let alone come up with an official sounding name like "Operator Assistance Network". When we first saw that line on the phone bill, we thought it was some kind of tax or surcharge. That's why we decided to expend a little gall of our own and expose the entire sordid affair, phone numbers and all.

how to hear phone calls

You too can be nosy and listen in to other people's telephone calls with a radio receiver. Depending on what kind of radio(s) you have, here are the things you can pull in:

Short Wave Radio: You need a general coverage receiver that is capable of receiving in single sideband mode (SSB) or has a BFO mode. Your antenna can either be the whip antenna on the radio or a long piece of wire, ten to fifty feet, running around your home or better yet, outside to a tree or pole. You will be able to tune ship to shore telephone calls within the following frequency bands (all numbers in kilohertz):

4357-4434,
6506-6521,
8718-8812,
13100-13197,
17232-17356,
22596-22716.

These frequencies are the shore station, which usually broadcasts both sides of the conversation. Transmissions are in upper sideband (USB) mode. Conversations may roll in from all over the world, especially at night, and will be in many different languages.

Some shortwave receivers can tune all the way down to the AM band. If yours does, check 1690 to 1770 kilohertz, where the old cordless telephone base channels are located.

Standard UHF/VHF Scanner: You can pick up cordless phones in your immediate vicinity, IMTS (old style car phones) in your general area, and airplane phones flying overhead. For the base stations, you'll usually hear both sides of the conversation, although sometimes the mobile caller won't be audible and you'll just have to imagine what they're saying. Use either the whip antenna on your scanner or buy an outdoor scanner antenna. These frequencies are listed in megahertz:

Cordless phones
46.610 to 46.970

IMTS car phones
152.510 to 152.810
(base stations)

Airplane phones
454.025 to 455.000
(land stations)
459.025 to 460.000
(airplanes)

The ECPA bans listening to car telephones. Cordless and airplane phones are governed by section 605 of the Communications Act of 1934, which says you can listen all you want as long as you do not divulge the information to anyone else or use it for profit.

800 Mhz Scanner: Newer

phone calls are

scanners cover all of the above mentioned scanner frequencies as well as the 800 Mhz cellular telephones (provided the manufacturer hasn't locked out the capability). Note that cellular telephones are of a wider bandwidth than most other scanner signals, and the average scanner may lose the peaks of some words, especially a high-pitched women's voice or a person screaming. For an antenna, start with the whip antenna on the scanner: slide it in all the way so that it is as short as possible (800 Mhz is a small wavelength, so shorter antennas are called for). Experiment also with angling the whip for better reception. Or purchase an outdoor antenna that is tuned for 800 Mhz. Or purchase a car cellular antenna and mount it outside your window (or on your roof).

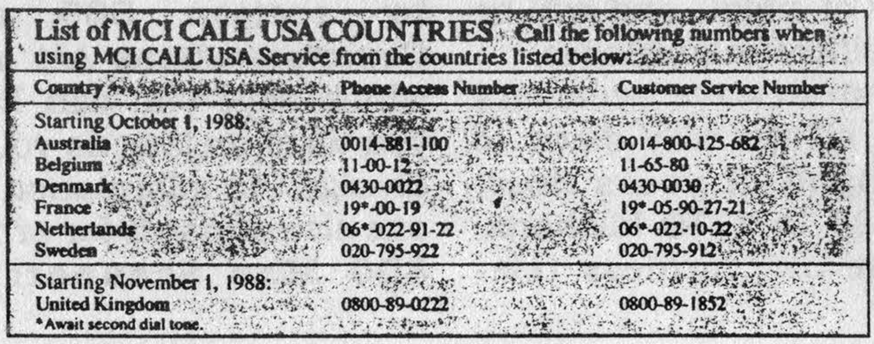
870.000 to 890.000
(base stations (cells) for the standard cellular system.)

890.000 to 896.000
(base stations for the extended cellular channels. Not in widespread use yet.)

As mentioned before, the unenforceable ECPA bans listening to cellular telephones.

Old Television Set: Some of the frequency space for cellular telephones used to be UHF TV channels 79 through 83. That's why newer TV sets have less UHF channels. If you don't have an 800 Mhz scanner yet, make sure there's an antenna attached (either the UHF loop or the UHF lead-in from an outdoor antenna), and try tuning across those channels. A continuous tuning knob will work better than the click stop kind. Cellular telephone calls on your TV set could be considered unwanted interference, but the law mandates that you turn your TV set off as soon as you realize that you are receiving protected communications.

Standard AM Radio: Haven't got any fancy radio equipment and don't want to buy any? If your neighbors are using the older models of cordless phones, you might be able to pick up the base channel at the far end of the AM dial (past 1600).



List of MCI CALL USA COUNTRIES Call the following numbers when using MCI CALL USA Service from the countries listed below:

Country	Phone Access Number	Customer Service Number
Starting October 1, 1988:		
Australia	0014-881-100	0014-800-125-682
Belgium	11-00-12	11-65-80
Denmark	0430-0022	0430-0030
France	19*-00-19	19*-05-90-27-21
Netherlands	06*-022-91-22	06*-022-10-22
Sweden	020-795-922	020-795-912
Starting November 1, 1988:		
United Kingdom	0800-89-0222	0800-89-1852

*Await second dial tone.

in the air

What might you hear on a car phone? We're not saying that anyone actually listens to this stuff and then writes it down for magazine articles, but if they did, it might look like this....

> I think that...the part of the problem is that they got -- they got a buyer for, for Kent. We'll just make it back in the commission for Kent. Now you understand that?
< Who'll just make it back?
> Huh?
< Who?
> Jerry, Larry, and you.

> What do you do with a group like that? You know. I mean what, I mean what, what do you with somebody like the deal?
< I don't know what you do anymore. I mean, the music is changing so radically it's hard to keep up.
> Yeah.
< It's hard to find out what to do it anyway.
> Yeah.
< You know?
> Yeah. Yup. How's the kids?
< How're the kids?
> Yeah.
< Kids are great, Bill.
> You got 'em a job yet?
< What?
> You got 'em a job yet?

> I feel bad for me. I feel bad for both of us. My heart hurts too. I love you.
< Who loves you?
> (osculating noises) I would kiss it if I could kiss your heart.
< (giggle)
> It was beating like a little thumper before.
< Really?
> (more osculating noises)
< God....
> A nice little orgy.
< Umm, I know. God you feel great down there tonight.
> Yeah I had it in, I was holding it differently.
< Oh. Felt wonderful.
> Did you notice that?
< Yeah. I told you it felt great, whatever it was you were doing.
> Uh huh.
< I could tell it was different, but I don't know what it, you're doing.
> Yeah. It was definitely different.... (pause) Want me to tell you what I did?

< Sure.

> I like squished it with my left hand. And I just left a space open for that leeeetle clitoris to stick out.

< You were squishing it? Cause it felt like you were pulling it apart?

> Well, at the same time I was, had the two fingers pulling it apart but the bottom of my hand, was like, squashing it in.

< Uh, well, that felt great. (pause) Oh. God I was horny.

> You're horny now?

< No, I was horny.

> Oh.

< Which one..

> No, the one we run last year was our art deco.

< Yeah?

> This is totally different. We're not talking about the same one. The one --

< Totally different is the difference between an eagle and an automobile. They're totally different.

> It's not.

< Sheesh. You're talking about a yoke treatment that comes down like a V, one is art deco, one is floral....

> Okay, then you know what I'm talking about.

< Of course I know, but you know, you're looking at it like through a microscope....

> No....

< And you're going to say it's entirely different but if you stand back and say "Hey...."

> Alright, watch what happens with this one....

< Well, I think we could do well with it, but it really is basically the same concept.

> I don't think so, not at all.

< You don't think it's the same concept?

> No, nope.

< Nah, then you're losing it.

> No I think they're all --

> -- and when can you give me an answer?

< Right.

> And it was very nice. But you can't, I mean she was on the phone with Brian this morning, and, and suddenly it was, it was the money thing. And I got on the --

< What's the money thing?

> You know, and I got on the phone with him and I said Brian, just, you know, come over here and look!

< But you could take almost

everything.

> I know.

< You know -- it's also bothering you in the background.

> No.

< Oh yeah.

> Not with Brian.

< Brian, he knows Brian all so well.

> Yeah, but Brian and he did not get along very well.

< Yeah, but Bobby seems has been to his head, you know, 'Be careful, you're gonna get screwed.'

> Yeah....

< You know, you know, uh ya know you hear it from, you know, either I get screwed or you're gonna get --

> Oh, I know, I know, but you know on the other hand after you talk to him for a few minutes he's coming over at one o'clock to work.... Howard?

< No bullshit about it.

> Yeah, but, uh, you know I mean they see, they see a lot of work going on down it's going to change people's attitudes.

< You know he -- if he wants to jerk -- you know, you know he could play all the routines they want, construction's slowing down right now.

> I know.

< And if they want -- you know, uh.... Lexington Avenue --

> I know.

< And Bergen Avenue.

> I know.

< And Old Bergen Avenue.

> I know.

< Uh, I, they just gotta understand, uh you know, I mean I gotta, what I gotta do is start going out there more to see him then.

> Uh huh.

< And, you know, doing my routine and say I know how to do very well with that.

> Right, exactly.

< They would give me a fucking break, we have some closings, we'll pay you, you know we're right around that time, we're closing, you just gotta wait a little while.

> That's right, that's right.

THIS IS THE FIRST IN AN OCCASIONAL SERIES ON POSSIBLE CONVERSATIONS THAT ANYONE COULD OVERHEAR. IF THIS HAD BEEN A N ACTUAL CONVERSATION, LOOKING AT THIS ARTICLE WOULD BE ILLEGAL.

Letters For

Some Ideas

Dear 2600:

After month's of agonizing over *2600*'s financial plight, I've figured out a way to return to the monthly format and solve another great problem that plagues BBS's all over the nation. How many times have you logged onto your favorite BBS and seen some message like this: "It has come to my attention that someone else is using *my* name, 'The Grim Reaper', on other BBS's. Well, whoever you are, I'm the *real* Grim Reaper. I was The Grim Reaper months before you came around. You better not use my name any more, or I'm gonna kick your $#&*@ ass!!! You better think of a new name dude!!!"

Well, the obvious solution to this common dilemma is to have a sort of "name registration", where individuals can register their alias with an authority -- kind of like your given name when you're born. And who else would be the most likely authorization but the hackers' and phreaks' choice -- *2600*! Think about it! You could charge each registration a nominal fee, like $3. For that $3, you will give the person a registration certificate, saying that he is the only one authorized to use a particular alias within a given limit, say, an area code. The person could get some little certificate to hang on his wall, and maybe even a patch to sew on his jacket.

So the next time the loser user logs onto the BBS, he can now proudly assert: "By the power of *2600*, I am the only Grim Reaper within the 212 area code. I am the only one certified and authorized to use that pseudonym. So be gone, you pagan!"

So, whadaya say? *2600* could be put into the black, and we would no longer have to put up with dueling 14 year olds. We have a unique opportunity to help solve the hackers' two most serious problems.

No thanks. There must be a better way to raise funds than to play big brother to dueling 14 year olds. Besides, how in the world would the user be able to prove that he/she was the one with the certificate hanging on their wall? Computers still offer a degree of anonymity. Let's all try to enjoy that while we can.

Articles & Boards

Dear 2600:

After having received your volume 4, number 10 issue, I was truly amazed! It's great to see a publication that is straightforward and informative. It wittingly caters to the novice, as well as those of us who hopelessly suffer from occasional periods of "hack attacks". Good job!!

I would like to inquire about submission of written articles, relevant computer news, newspaper stories, and the like. I believe I have or can obtain enough data to "publish" at least one article on a minimum quarterly basis. Also submittable would be a collection of "postings" from the area networks which would be of worth to your magazine.

Next on my list is the hope of being allowed to operate a Greater New Orleans branch of *2600* Magazine BBS. I know of *many* people and users who would be more than happy to benefit by logging into a system like such. A BBS of the like would offer its users a wealth of information that would otherwise be inaccessible, or worse yet, unnoticed! As I soon will have a phone installed with a few *extremely* advantageous services such as call forwarding and call transferring, I will also be able to link users to systems that would be out of their reach *but within mine!* I think that the combination of what a *2600* Magazine BBS could offer, plus a bit of effort on my part, would bring about great results.

SW

You can contact us with your BBS ideas by calling 516-751-2600. We're also always asking for unsolicited articles, so if you have something you think we might publish, send it in.

Need Info

Dear 2600:

I understand that the Telecaption Adaptor II available from Sears can be extended with a few parts to have an RS232C serial output port for a computer. I would like to find out how to do such a modification so that the TV subcaption output can be displayed on a Teleprompter with RS232 input. This would allow people who are both hearing and sight impaired to understand TV. My grandmother cannot see the tiny letters that the TCA II generates on the screen. I would appreciate any information on how to accomplish this modification.

Handel

AT&T Nightmare

Dear 2600:

Our small liberal arts college recently switched over from its

The Winter

old crossbar system to the AT&T System 85 early this year. In the old days, you subscribed to Wisconsin Bell (like all Wisconsin residents), had your name in the phone directory, were available through directory assistance, and could use your long-distance service with the 1+ option. That has changed since then. If technology is supposed to make life easier, it doesn't and it also makes it a hell of alot more expensive.... To make a long distance call, we now have to dial the 800 port (I use Sprint) and use a calling card to place the call. For those of you who use software for your modems, try programming a 20+ sequence! Then we also are charged a 50 cent surcharge for placing the call! And if you're like me, that really adds up. We are unable to call 950's, "toll free" Wisconsin Bell lines, and we are unable to turn off call waiting for an incoming call. Good if you are trying to run a BBS from your dorm room. There are only 37 outgoing lines, and 27 incoming. So during normal business hours (the school's business office is also on the system), you will be unable to place a call! Someone from AT&T also forgot to program all of the reachable prefixes in our area! Even some of our faculty cannot call home! For a system that is supposed to be "smart", it sure isn't. If I were to call myself using the prefix that the school is accessible through, the phone system doesn't even know to just use an internal switch. Instead it goes ahead and wastes an outgoing and incoming line while I talk to myself. So to prove to the school that something needs to be done, we're getting 37 people to call themselves during busy business hours, and make the system paralyzed...for about 4 hours. That should teach them what they refuse to listen to. Like all systems, no one cares until it happens to them....

Cray-Z Phreaker
Skunk Works

The bug you're about to exploit is probably the easiest part of the system to fix. All they have to do is block out that exchange like they've blocked out others. But the point is you have to get the college and the phone company to listen to you, the end user. You must do whatever you see fit. This means being loud and specific as to what problems you're faced with. Remember, you have the same right to telephone service as anyone else in this country. Being at a col-

lege does not mean you're signing away this right. Demand answers and if you don't get them, make sure everybody knows it.

And a message to AT&T: This is the second time in as many issues that we've heard major complaints about your System 85. Last time it was the House of Representatives. Who will it be next?

Call Forwarding

Dear 2600:

I'm hoping you may be able to answer some questions regarding the phone company's availability of call forwarding.

As it stands, in order to activate call forwarding, you must have the service on your line and you must activate it from that line. It must be deactivated from the same phone that it was activated on.

My question is this: is it possible to forward Phone "A" to Phone "B" from Phone "C"? Also, is it possible to have a pay phone forwarded to your location?

JH

There are remote call forwarding devices available that allow you to change the number you're forwarding to and to cancel call forwarding from a remote location. We talked about these in our last issue. So far we haven't seen a phone company offer these services. Regardless of who offers it, though, there is another potential security risk here.

With regards to using forwarding on a payphone, there are two answers. The first is no. That is, according to the phone company. After all, why would anyone want to use forwarding on a payphone? It's simply not possible. The other answer is yes. Of course, it's possible. Hackers have done it by using the phone company's computer. And we don't doubt that law enforcement has made use of it on occasion. What better way to trick a drug dealer or kidnapper calling a payphone?

Observations

Dear 2600:

Seeing how you have published updates to the 800 exchanges that are owned by IC's, here are some 800 exchanges that belong to other companies, as well as some of the same companies (MCI, Sprint, etc.). These all work from my NPA, and I live in the midwest. I know that one carrier (LYTEL) is a re-seller of long distance lines to FG-B carriers in my area. Anyway, the list:

800 + NXX

We Really Like

373	Teleconnect
383	Teleconnect
456	MCI
472	AT&T
589	LYTEL
636	Conquest Long Distance
668	AT&T
686	Conquest Long Distance
728	Teleconnect
747	Teleconnect
798	Teleconnect
829	Sprint
869	Sprint
873	MCI

These are the exchanges that I have found that were not listed in any issue of *2600* under any company. There may be more, since I compiled this list a few months ago. Also, Teleconnect in this case is not the same company that runs *Teleconnect* Magazine, I am told. I can usually tell by listening if the exchange is owned by an IC, as there seems to be more noise and static on the connections and in the background than there is with AT&T 800 numbers. Also, in my area at least, the connection time for an AT&T 800 number is less than for an IC-owned 800 number. Western Union's service used to be such poor quality in my area that when I dialed 10220# (their equal access override), I could hear the noise being cut for ANI and called number outpulsing. This also was the same for Allnet.

Speaking of Allnet, I am a legal customer of theirs, with dial-up service. When I got my authorization notice in the mail, I discovered that my code had been put in on Allnet's 800, 950, and local FG-A dialups. On the 950 and local FG-A node, I could use my 6 digit code "as is", but with the 800 "Travel-Mate" service, I must enter my 6 digit code, plus my three digit PIN. (By the way, Allnet used to use some type of formula to derive customers' PIN numbers. This formula used part of the customer's exchange as the first digit of the PIN. I am just mentioning this for the sake of information, as they no longer use this method, according to customer service.) I am less than happy with Allnet's service -- they are raising prices in my area for both dialup and equal access dialing. Also, they cannot seem to get their records straight. Somehow I was signed up with Allnet as my PIC even thought I did not choose them. I talked to customer service about it as soon as I found out and they told me the problem would be fixed. Soon afterwards, I received a notice in the mail telling me that I had been disconnected from Allnet. However, to this day, I am still connected with Allnet and they cannot get the bills straight. They send the bill for 1+ to my address for dial-up bills. I have called them several times and still they cannot fix this.

Also, to top things off, we still received the charge from our local BOC to pay for the disconnection from Allnet even though we are still connected. I have called customer service a number of times and they don't seem to want to help. I have considered dropping Allnet because of the several things they have done, but I am still a customer of theirs. The only good thing about Allnet is that they have a 45 second buffer zone that is used when a call is connected. So if you can keep a call's time less than 45 seconds, it won't show up on your bill. I imagine that sooner or later they will get the equipment to detect answer supervision, but it looks like it will be later.

In the Spring 88 issue you published a list of BOC routing and system codes. You asked if anyone knew how to use the Mexico function of RQS. You can use this with a Mexico NPA, such as 905. Just use 905 as the NPA and use two Mexican exchanges in the exchange information, and RQS will tell you the rate. If you want to try this out, a valid exchange in Mexico is 621. So if you use 905+621 and get the rate information for an intra-office call (to the 905+621 exchange), you will get a local call message.

Also, a note to Telenet ID users, according to Telenet Customer Service, the cost of getting an ID is $24 a month, $18 a connect hour, and the bills are itemized (shows that the ID user connected with). So if this information is true, then no wonder Telenet ID's always die when people use them illegally. Also, Telenet has a new type of access management system called TAMS (I am not sure what it stands for) which keeps better track of network usage.

Phantom Phreaker

An increasing number of IC-operated 800 numbers actually have better sound quality than AT&T's. They also have more sophisticated caller identification features.

If you have a letter to send to us, drop it in the mail addressed to: 2600 Letters Department, PO Box 99, Middle Island, NY 11953.

What It's Like To Be

by E. Solomenko
(reprinted from Pravda)

I first came across her when as an inter-city telephone operator in Novosibirsk she tried long and hard but without success to put me through to Ashkhabad.

Her efforts were in vain. "I'm sorry," she said, "I'll try via Mara."

Getting through to Mara was no problem. "Hello, Mara? Can you help me get a line to Ashkhabad?"

The reply was anything but sisterly, "Dial it yourself!" Then they cut her off.

I reflected sadly that the lack of solidarity in Mara was a far more common approach than that of my Novosibirsk guardian angel of the telephone exchange. I remembered how on a previous occasion I had also been trying unsuccessfully to get through to the elusive Ashkhabad, when the operator told me that there was a fault on the line.

Just in case, I decided to try getting through without her help, by dialing direct from the telephone box. Miracle of miracles -- the inter-city code worked and I got through. The operator had told me there was a fault in order to get rid of me.

Ashkhabad was notoriously difficult to get a line to. Yet now her senior colleague was trying again and again to connect me and I could hear her saying to the girl next to her (she had forgotten to switch me off) that she hardly had any voice left from shouting down the line to Ashkhabad.

At long last I heard the voice of my friend, the artist Durda Bairamov, over the line. We both had to bellow in order to be heard; the line was terrible. The operator's hoarse voice broke in as she started relaying my questions to Durda and his answers back to me. I felt very touched by her concern and just had to find out who she was.

Her name is Valentina Efimovna Vdovina and she works in what they simply refer to as the "inter-city", which is one of the country's largest telephone exchanges, connecting the Urals with Kamchatka and Kuril.

So what is Valentina Efimovna like?

"She's a conscientious worker," said the supervisor, T. Vereshchak. "She never goes home until all the calls that have been booked have got through. Sometimes she sits on into the night long after her shift has gone off duty. We have a lot of good operators here, but we all take our hats off to Valentina."

Then who should come into the room but Valentina herself. About 40 years of age, small with a round face and short hair and very kind, homely eyes. She sits down, obviously tired. Before lunch today she was working on eight calls at once.

Her job isn't exactly a piece of cake. She only has one day off a week and has lost count of the number of national holidays she's spent sitting in front of the switchboard. She works six hour shifts doing what amounts to a juggling act with both hands, connecting and disconnecting plugs from the switchboard.

A Soviet Operator

Then there are the operators' fetters, the earphones with mouthpiece attached. Just try spending a whole shift wearing those things! You soon get bells ringing permanently in your head from the constant noise, and this leads to headaches. Your voice suffers too from the constant shouting to make yourself heard over bad lines.

It is no accident that state legislation allows for early retirement in this job. After ten years in the inter-city, you can retire on full pension at 50. Only a few soldier on for longer. Lilya Gleikh, Vera Raeva, team leader Elsa Vasilievna... Ludmila Ivanovna Gorbatova has served her for almost a quarter of a century and has risen from operator to manager. Other girls come here straight from school and don't last two minutes.

"I'd get out myself," sighed Valentina Vdovina, "but I love my work. I think of it as helping people to meet each other. It's as if I have a hand in their fates, even if only for a minute."

I said that no doubt she overheard many conversations between callers, not on purpose, of course, but how else could she check the quality of line and make sure that they could hear each other, how else could she let them know that their time was almost up?

Whether she likes it or not, the operator must be party to other people's secrets, to their joys and sadnesses. There must be calls from sons returning from the army, calls to announce the birth of a grandson, to say that somebody has been put in prison or that someone else has had a heart attack.

Sometimes they overhear whole conversations, late at night or on holidays when there are fewer calls going through. During normal working hours they only have time to quickly listen to check that everything is OK. Twenty seconds for each call and on to the next one.

A local call comes in. "Please put me through to Lesosibirsk as quickly as possible, my dear!"

"What number do you want?" Valentina asks.

"I'm afraid I don't know," sobs the voice.

"Please don't cry. Let's try to think how we can find the number. Who do you want to ring there?"

"My daughter's had an accident there," says the woman's tearful voice.

"Don't worry. I'll get through as quickly as I can. I expect the surgical ward of the hospital there will be able to help."

She got through to her colleagues in Krasnoyarsk who gave her a line to Lesosibirsk. From there she got through to the hospital and then to the doctor in charge of the surgical ward.

"Hello, this is the Novosibirsk inter-city exchange. Has there been a young woman admitted following an accident? There has? Hang on a second, I'll connect you to her mother."

Later the mother rang Valentina,

Operating In The

this time crying with relief.

"Thank you my dear. I can't tell you how much you helped me. I don't know how to thank you for all you did."

She doesn't have to thank her. For Valentina the main thing was that the woman found her daughter, knows that she is alive and will get better. That is the best thanks she can get.

In the course of her work she comes across all sorts of different people. Sometimes during the busiest time, when all hell is let loose with ten calls going through the switchboard at a time, you suddenly get an irate caller bursting in saying: "How much longer must I wait? I haven't got all day you know. If you don't pull your finger out I'm going to complain."

"Sometimes we even have difficulties with other operators," explained Ludmila Gorbatova. "We can never get through to the Baku inter-city exchange, the operator on duty never answers. She's either asleep or has gone off somewhere.

"When she does finally answer she shouts something in Azerbaidjani down the phone and hangs up. After which you can never get back through again. We have sent a complaint to the USSR Ministry of Communications and the Baku inter-city exchange, but without result."

Vdovina says that she doesn't very often come across operators like the one in Baku. The other Siberian operators in far eastern exchanges are all considered to be "one of us" at Novosibirsk.

Valentina started off by working on the Krasnoyarsk district link and now is on the Khabarovsk line which includes the whole of eastern Kazakhstan plus a good chunk of Novosibirsk province.

She is an important link for miners, people working on the gas pipeline project and the agricultural industry. When there is an accident on the pipeline for example, or problems with drilling. When a couple of teams are needed urgently elsewhere -- all this concerns her and she does her best to help.

Let's take, for example, the Novosibirsk Pipeline Construction Trust. She knows as much about their business as its dispatch clerk, Vladimir Ivanovich Golitsin. She knows that the Trust is involved in pipe projects in Belgo and in Lower Tambovka, in Yagodnoe and in Krasnoyarsk.

"Hello, Mr. Golitsin, I'm putting you through to Belgo."

"Hey, Valosha, what about a hello first? How are you nowadays?"

"Hello Vladimir Ivanovich. I can't really talk for long now, the supervisor's here and I'll get told off for chattering!"

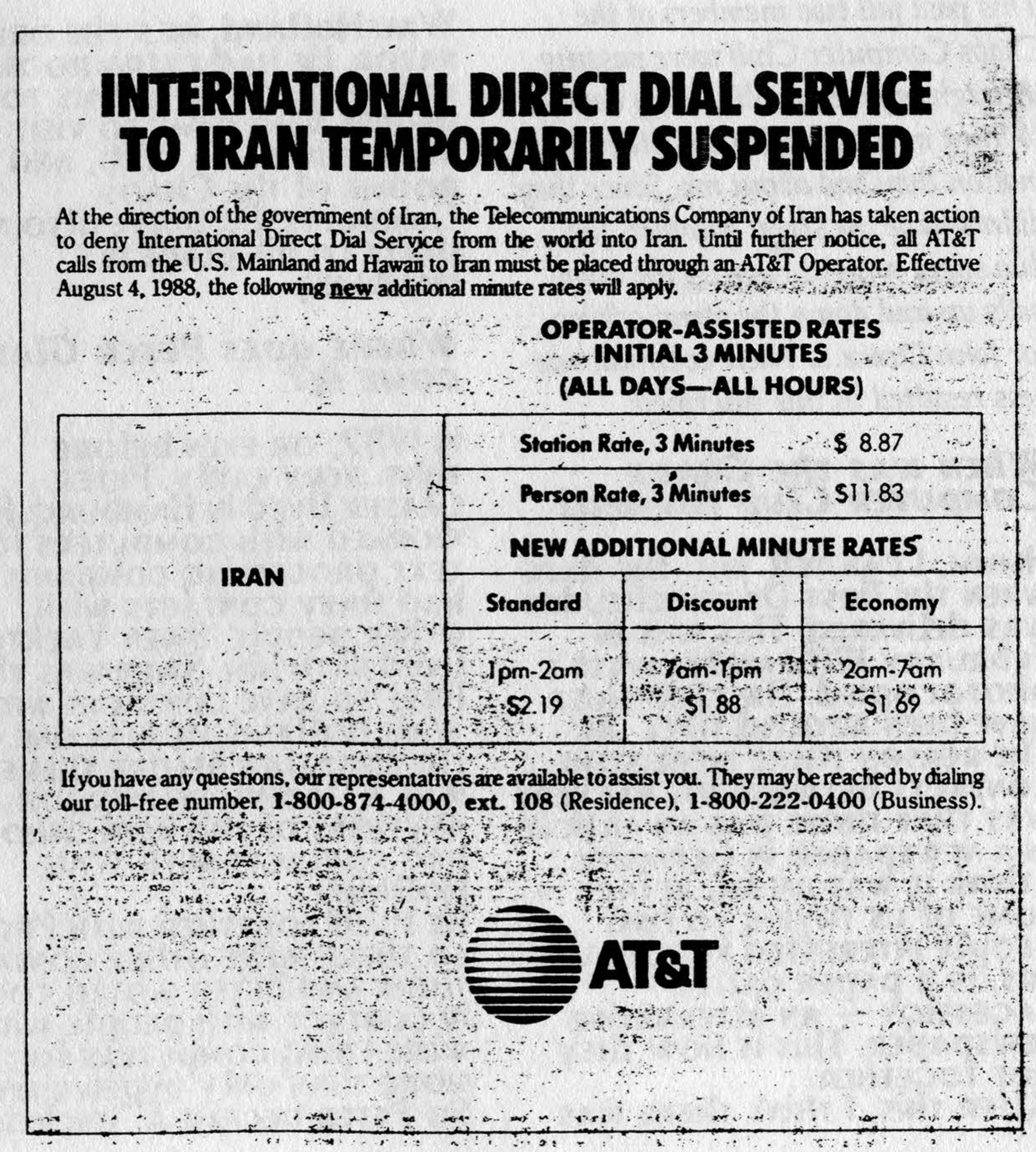
The supervisor, Taisiya Aleksandrovna just smiles. "You seem to know the whole country, Valya!"

"Not quite," laughs Valentina, "only half!"

Her son Seriozha more or less grew up in the exchange. When he was in the fourth class he was told to write a composition called My Future Career. He wrote: "I want to be a switchboard girl." When his mother saw it, she laughed and told him to change it to "man". He looked at her from under his brows and said: "What do you mean, 'man', when they're all girls?"

Over the past two years she has not been very well. The strain of the job is starting to tell. Not long ago she did a break, but now her short, 18 days of holiday are over and she is back at work -- how could they manage without her? She hurries to light her beacon for the Sea of Anxiety, the Sea of Joy, and the Sea of Loneliness.

Tomorrow I shall have to ring Khabarovsk. I'll dial the inter-city and book my call. And how good it will be to hear that friendly voice saying, "Did you book a call to Khabarovsk? Putting you through now."



INTERNATIONAL DIRECT DIAL SERVICE TO IRAN TEMPORARILY SUSPENDED

At the direction of the government of Iran, the Telecommunications Company of Iran has taken action to deny International Direct Dial Service from the world into Iran. Until further notice, all AT&T calls from the U.S. Mainland and Hawaii to Iran must be placed through an AT&T Operator. Effective August 4, 1988, the following new additional minute rates will apply.

OPERATOR-ASSISTED RATES
INITIAL 3 MINUTES
(ALL DAYS—ALL HOURS)

IRAN	Station Rate, 3 Minutes		$ 8.87
	Person Rate, 3 Minutes		$11.83
	NEW ADDITIONAL MINUTE RATES		
	Standard	Discount	Economy
	1pm-2am $2.19	7am-1pm $1.88	2am-7am $1.69

If you have any questions, our representatives are available to assist you. They may be reached by dialing our toll-free number, **1-800-874-4000, ext. 108** (Residence), **1-800-222-0400** (Business).

AT&T

an interview with

by John Drake

Not much is known about the Chaos Computer Club, except for the abundance of scary "you should hire me because of hackers like them" tales peddled by computer security consultants.

Further hype about the "mythical hacker elite" has also been perpetuated by the worldwide media coverage when a story is picked up by a major news service.

This past fall two members of the Chaos Computer Club were passing through my metropolis. They decided to hunt me down with the little information they had about me. Since they didn't have the street number, the duo spent a night ringing the doorbells up and down the street asking for John Drake.... Their eventual success resulted in this interview.

When was the Chaos Computer Club formed?

Hmmm, I can tell you the date when the first Datenscheuder was delivered. This was in February 1982 and it wasn't photocopied. The club must have been around since '81. The reason there were some contacts between the hackers was that there was an article in a newspaper in Germany.... I think it was an ad, in fact -- some of us trying to find people interested in computers, in a paper called Tagensign -- an alternative newspaper. This is how they got together.

After this, I think there was an article about hackers -- people who work with computers and that mentioned the Datenscheuders. It was in Der Speigal, like Newsweek here, or Time, and so suddenly many people phoned and wanted to get the Datenscheuder. Then from there the second issue of Datenscheuder was printed a lot, then the Chaos Computer Club.

Who then started the Chaos Computer Club?

Wau Holland, he's the originator. He had extra rooms and he gave the rooms to people who came to visit him before it was a club, and the rooms of the Chaos Computer Club are also next door to his place in Hamburg.

Where does Peter Glaser come in?

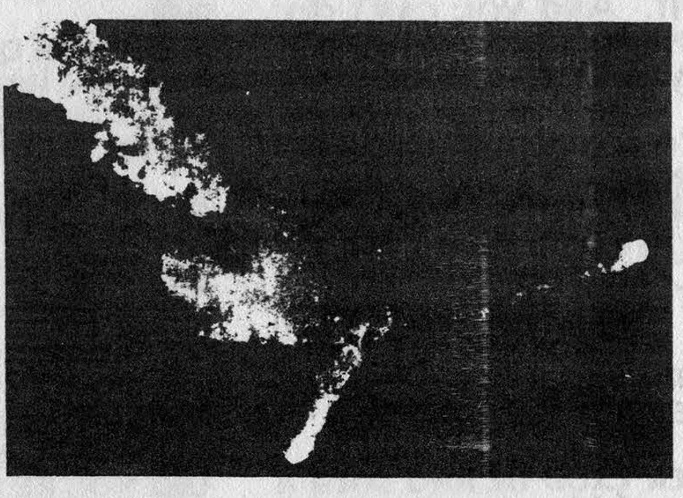
In 1982, or even before that...very early. Peter Glaser lived in Hamburg. He worked with computers for a text processing company. He had many contacts with other people. Swen Yacktoff lived with him. Swen was the first to have contacts with Wau Holland. He was one of the first, far before there was a Datenscheuder, or anything of this kind, who had contacts with Wau Holland.

He lived together with Peter so there were other contacts there and Peter would come in contact with people who were using computers for more than only typewriting. So Peter became a "hacker". I

the chaos computer club

don't know if he is really a hacker....it's a silly word. When he got a modem for a birthday present from someone from the Chaos Computer Club, from that time you only see his back. Yes, when you wanted to communicate with him you had to buy a modem yourself. But, that's over now, he only goes online very seldom.

Hamburg (DPA) ... ARIANE - so ein Sprecher der NASA - sei wohl nur deshalb so hervorragend gestartet, weil Hacker im Bootsektor der Rakete Verbesserungen vorgenommen hätten. ...



Chaos Computer Club, Schwenckestr.85, D-2000 Hamburg 20, Telefon: 040 - 490 37 57, BTX *CHAOS+
Mailboxsystem CLINCH 040 - 651 64 75, via Datex-P 44400090314, GEONET:GEO1:Chaos-TEAM

How is the Club set up in relation to Datenscheuder?

Datenscheuder is the paper of the club.

How is the club organized?

That's very hard to say because as an officially registered club it's only been a year now. Before then it was just the Chaos Computer Club. But then you need someone for the bank account and you need a registration.
It's a galactical connection without structures. Anyone can come without having to be a member.

How many people receive the Datenscheuder?

We are printing two thousand, I think, but only about 800 to 1000 are actually mailed.

How has "the press" looked at the Club? You always see reports about the Chaos Computer Club breaking into one system or another....

When you give them (the press) something to eat, they all come running.

Examples?

When you hear we have just gone into a databank, everyone from the German press will come and write about it. In the beginning this was very fine and some good actions came about because of the Betax hack...now there is the

the chaos

NASA hack which is very famous.

But often there are journalists who think "What can we do in our newspaper?" and then they say, "Ah yes, something with computers -- let's phone the Chaos Computer Club. Is there anyone here with the number?" Then they phone and say, "Please show us some hacking, let's see how you do it." And you can't do it because it is forbidden in Germany. It's not the reason why the club exists: for journalists to let people know there are hackers.

When a byte somewhere goes wrong they always phone the Chaos Computer Club, because they think we can fix it or we know what has happened or who did it.

Someone once told me that because of the Chaos Computer Club he had sold a lot more of his security software and he thanked us.

Is the main aim of the group computer literacy or is there a faction inside the group for hackers?

There are many different people who think of many different aims of the club, some of them socially acceptable ways of working with computers. Some of them are hackers but not all of them. We are not hackers.

Is it then a straight computer club?

No, it's not a normal computer club. It's more of a Chaos Communications Club than Chaos Computer Club. I don't think you need the computer. It's more for people who think more than hack, perhaps. There are also hackers in the club, sure, that's a bit of the problem because hackers have different interests than people like us who are more interested in communication and art. Whether they're just freaks that know a lot about the technical side....

There are other people into real live hacking, like showing press passes to get into things, that's real hacking.

What type of laws exist in Germany to deter hacking?

At the moment when you change something in someone else's computer, it's already an offense. So when you login and you're not supposed to login, you change something because it's reported somewhere that you have logged in. So you have already changed something if you follow the law strictly. I think that they are still working on these laws.

computer club

Has anyone been caught and fined on a hacking charge?

The only thing that I can think of is Steve in prison, but he hasn't been charged.

Can you give me some examples of media distortion?

There was this bit with a bank in Hamburg, on a videotex system in Germany. It has many many bugs and many mistakes in it and when you have an overflow of data, anything could happen.
So in this way they found out the password of this bank in Hamburg and they used this, and then the Chaos Computer Club ran a section of information pages on the videotex system. They also have a movie in there which you can look at but you have to give a donation for looking at the movie -- five dollars, which is the maximum sum for looking at a videotex page.
Well, they made the bank look at this page over and over again. They wrote a little program so it was always calling it back again and had it run over the weekend so no one from the bank was there to stop it. In the end it was 150,000 marks worth of donations from the bank to the Chaos Computer Club. The Club could have claimed the money from the bank because there are no laws saying that this wasn't ok. They didn't, but they showed the national data security office what is possible. The bank was very thankful for the hint.
The host operator of the system said, "It's only because of the Chaos Computer Club that the Betax videotex system is a flop." They were telling us at the demonstration of Betax that it was because of the Chaos Computer Club that people won't use it.
Also, whenever there is a show of the Betax videotex system, people call up the Club's movie on the demonstration accounts.

How does the phone system work in regard to modems? Is it digital or a clunking mechanical system?

You still have the clunk, clunk, clunk system in most towns. They have just started to change to the digital system.
If you want a modem you have to buy it or rent it from the post office. Or you use a Hayes modem which is illegal. The modems from the post office aren't very powerful. There isn't any good software to work with them and they're very expensive.
In Germany it is forbidden to do anything yourself with the telephone line. There is a joke that you even need permission when you use a pen to dial the phone.
If you need a longer cable you have to go to the post office and pay 65 marks and fill out a request form for a longer cable to your telephone.

west germany's

So phone phreaking is not a hot subject in Germany?

There are sometimes people who try to make blue boxes or things of these kind but I don't know if they work. There was one guy we knew who had a thing like this, but he disappeared into prison or somewhere. We have to try...maybe it will work when the new systems are installed. Telephone calls are very expensive in Germany, especially long distance calls and so it would be a useful thing.

We are charged for all the local calls in units of eight minutes in the day and 12 minutes at night.

What happened to Steffen Werrney when he went to France?

Steffen was invited to a security congress to report about what happened with NASA and to explain what is possible in these networks. He was arrested right away when he arrived at the airport in France and questioned for 24 hours.
They kept him there waiting while they had absolutely no evidence whatsoever that he was in any way involved in the NASA story.

What actually happened with NASA as opposed to what the newspapers said?

They're not members of the Chaos Computer Club. They were one year working for a company and suddenly they found out that they were in the NASA network. After a while of working inside there, they one day began to understand that it was very dangerous.
There are stories about the CIA -- they don't ask questions, but shoot first. I don't believe these stories myself, but then I think the Americans must be silly....
Then one day they phoned and came to the Chaos Computer Club and said to the people there, "We have some computer printout and we don't want to be killed by it. What shall we do?"
Steffen and Wau said OK, keep quiet and we will use our contacts. Then the machine started. They tried to give information to the CIA via the German Secret Service. They saw that one week later the account was still working. They gave notice to the company that was manufacturing the terminal software. Then there was a new version distributed that still carried the same mistake.

What did the communication software allow you to do?

It allowed you to look at the user list. Usually it tells you that you have no permission to look at it or do anything there. It gave the warning in the program but it wouldn't cut you off. You could go farther despite it saying you couldn't.
So they went in and gave themselves privileges in the system, and they put in these trojan horses -- programs

"computer hackers"

THAT WIPED OUT ALL TRACES OF THEMSELVES IN THE SYSTEM SO NO ONE KNEW. IT ALSO COPIED ITSELF INTO OTHER SYSTEMS ON THE NETWORK AND BROUGHT BACK INFORMATION ABOUT PASSWORDS TO THE KIDS. THEY HAVE BEEN IN 135 DIFFERENT SYSTEMS.

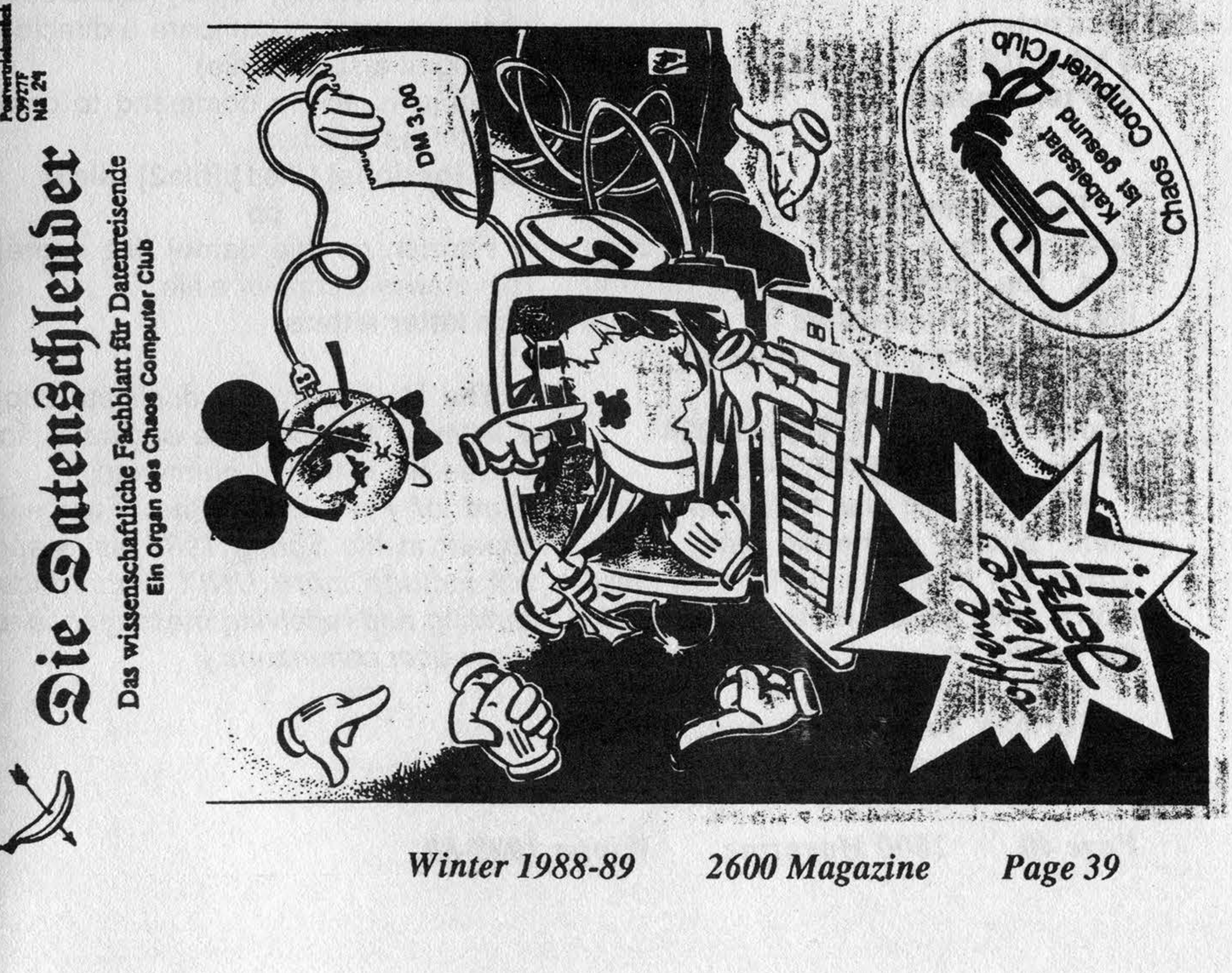
Die Hacker Bibel I & II, what is it?

You find some reprints of some American stuff in it (TAP), complete reprints of old Datenscheuder, and some articles you will only find in the book. You can find this over the counter in any bookstore.
I think it has an ISB number. Die Hacker Bibel II is due soon. It's been printed. We're waiting for Steffen to send us copies. Die Hacker Bibel III is now being worked on.

258 pages softcover
ISBN 3-922708-98-6
Published by Der Grune,
Zweig 98, West Germany.
Cost 15 dollars US approximate.

- *Original Material written for Bibel.*
- *Photocopy art/humour related to computers and hackers.*
- *News clippings and articles from various sources.*
- *Includes reprinted article about Hackers Conference.*
- *Reprints from Datenscheuder.*
- *Early YIPL 1-22 reprints and TAP 23-27.*
- *About 40% of the book is in English.*
- *A good reason to learn German.*

Chaos Computer Club:
D-2000, Hamburg 20 or
Schwenckestrasse 85
West Germany
01149404903757, 0114940483752.



UNIX HACKING

(continued from page 17)

wd" command as shown below:

```
$passwd
Changing password for john
Old password:
New password:
Retype new password:
$
```

This will only work when the password has aged enough.

ps

It's sometimes necessary to see what command processes you are running. This command lets you see that. The format is: ps [-a all processes except group leaders] [-e all processes] [-f the whole list].

```
$ ps
PID  TTY  TIME  COMMAND
200  tty09 14:20  ps
```

The system reports the PID - the process identification number which is a number from 1-30,000 assigned to UNIX processes. It also reports the TTY, TIME, and the COMMAND being executed at the time. To stop a process enter:

```
$ kill [PID] (in this case it's 200)
200 terminated
$
```

grep

This command is important when searching for a word or words in large files. The format is: grep [argument] [file name]. It searches for a file that contains the argument specified.

```
$ grep phone cathy
phone   michelle  (718)5551234
phone   cindy     (718)5553456
```

What this did was to find the argument "phone" in the file cathy. If the argument consists of two or more words, then it must be enclosed in single quotes.

mv

Format: mv [file names(s)] [dir name]. This renames a file or moves it to another directory.

```
$ mv letter letters
$
```

This example renames the file letter to letters, thereby deleting letter. If you want to move files then you would enter:

```
$ mv /usr/john/pers/capital /usr/john/michelle/capital
$
```

This moves the file capital to the directory named michelle.

diff

Format: diff [file name] [file name]. This shows the difference between two files. Output of this will have something like 4,5c4,5 then it will display both sets of files on the screen. The 4,5c4,5 means that you must change "c" lines 4 to 5 in one file to line 4 to 5 in another.

Options for using this command are: -b (it ignores blank spaces), -h (compares it quickly), -s (reports files that are the same), -S[file] (this is used when you want to compare a directory starting at a specific file).

There is also a command to compare 3 files which is:

```
diff3 [options] [file1] [file2] [file3]
```

cp

Format: cp [file name] [file name]. This makes a copy of a file.

```
$ cp letter letters
$
```

The file letters is a duplicate copy of letter. In this case the original is not erased like in the mv command.

(End of Part One. Part Two will appear in the Spring 1989 issue and will include more UNIX commands, sending and receiving messages, and super user commands.)

2600 Marketplace

WANTED: Text files/ Countlegger/ Phrack news clippings on hackers, phreaks, etc. from newspapers and magazines. Willing to pay or trade. Send a list to KH, N. 11107 Roundup, Mead, WA 99021.

WANTED: Any hacking programs for the Atari ST. Will trade. Also in need of good blue box plans. Would love to hear from other persons interested in P/H from Lexington, KY. Aristotle, 606-258-2219.

COMPUTERIZED LEARNING USER'S GROUP, ELECTRONICS is for those interested in learning electronics and related technologies as well as those interested in developing, evaluating, sharing, and selling hardware and software to do so. Write CLUGE, 207 East School Street, Kent, Ohio 44240-3837 or call 216-678-4611.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

WANTED: Red box and/or blue box, tone chips for making boxes, Macintosh software for trade via mail or modem and vending machine lock-pick gun/tools. Douglas, PO Box 8022, Richmond, IN 47374.

FOR SALE: 3 Comtech model 550 Satellite Video Receivers. Best offer, first come, first served! Send reply to either dtroup@carroll1.uucp or send real mail to: DTROUP/Room 205st, 221 N. East Ave., Waukesha, WI, 53186. Skunk Works!

FOR SALE: Various UNIX manuals/books. For more information, write to Seth K., PO Box 245070, Brooklyn, NY 11224.

I WANT TO START a newsletter devoted to petty crimes, tentatively titled "For Informational Purposes Only". Please send me info, clippings, on how to rip-off vending machines, free postage, free photocopies, sneaking into movie theaters, etc. Tim Cridland, PO Box 85874, Seattle, WA 98145.

WILL TRADE: My Texas Instrument Silent 700 Series Portable Intelligent Data Terminal (like new) w/full documentation for any hacker software for IBM compatible computers. Ted K., PO Box 533, Auburn, NY 13021-0533.

COMPLETE RANGE of Commodore 64 hack/phreak software. All tested and debugged. Many advanced applications. Call THC-][BBS at 604-595-0085 and leave feedback to the sysop for more information.

TAP BACK ISSUES, complete set Vol. 1-90 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid via UPS or First Class Mail. Cash/MO sent same day, checks to Pete G., P.O. Box 463, Mt. Laurel, NJ 08054. We are the original; all others are copies!

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market (also known as the lobby with the tables where all of the weirdos hang out). Located at 153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info.

Deadline for Spring Marketplace: 3/1/89.

HARDWIRING

by Dr. Williams

One of the most obvious ways of obtaining free telephone service is through "hardwiring" -- that is, directly connecting a phone to somebody else's line without their knowledge. This can be accomplished in a few different manners. One technique is just to hook up a phone to the exterior of a house or business. Another way, canning, is a little less blunt. Any dime store phone can be hooked up, and walaa! Free telephone service is yours just for the begging.

There are basically two types of exterior phone boxes that are used for homes and small businesses. The older ones are a pukey green color, are square, and have four terminals inside: two for the grounds, and two for the charged wires. These are kept closed by a long bolt. The newer ones are rectangular and have a phone jack inside of them. They are kept closed by a lid. There is only one tool you'll need, and that is a touch tone phone. The ones where all of the components are contained in the headset are the best for this. Take the cord, cut it in the middle, and strip the wires on both halves. There should be four wires: a green, red, black, and yellow. The green and red ones carry the current, and the black and yellow are the grounds. There could be some variations in the colors of the wires, depending on the phone, but there should always be two grounds and two charged wires. After stripping the wires, put an alligator clip on the green and red wire on both halves. Putting one on the grounds is a good idea too.

Now you have what it takes to connect up to any phone box. On the older ones where there are just four terminal posts, you take the headset and connect up to the terminals via the alligator clips on the headset. You won't need to use the other half of the cord with the phone jack since there is no place to hook it up. You may also have to bring some vise grips to unscrew the bolt which holds the box closed. Sometimes, the colors of the terminals aren't marked, so it will take some trial and error to find the two live ones. On the newer boxes that have a telephone jack inside of them, you use the other half of your cord containing the jack to plug inside of it. Then you connect the alligator clips together on the headset. This should be no problem to open since they are held down with a plastic lid. Easy, isn't it! One note, though. There may be other variations out there. From my experience, these are the most common types of boxes.

There are some drawbacks; relationships are always two-sided. The good points are that it's easy (it beats hacking out codes to the local extender at the pay phone) and, since most residential areas still use AT&T as their primary carrier, you can call anywhere in the world. Some other long distance carriers have limited calling areas. The drawbacks are, first, you have to do this at night -- like, 3 or 4 am. If you do this, you always run the risk of getting caught. Some neighbor might think you're a prowler. You should therefore dress in dark clothes and not carry any identification with you. There is also a limited amount of things you can do. After all, you can't call up your relatives or too many of your friends at that time of day.

There is a wealth of locations where one can try to hook up. One spot is housing construction -- going up and coming down. Sometimes, when houses or apartments are being built, the phones are connected before construction is complete. I've also seen cases where people move out and the phones are not disconnected. Once the people lived in a mobile home and they moved out, leaving a vacant lot with a utility pole. Well, lo and behold, the phone was still connected. The phone company didn't disconnect it until about seven months later, and that was after practically everyone in the neighborhood had crank-called people in Japan and Australia. You can also try rural neighborhoods late at night, although using your own probably isn't a good idea.

Small business clusters or industrial centers are also good spots. These usually have the green boxes clumped together in lots of four. Late at night, no one is around, so it's only a matter of hooking up. I'm talking about those places where a company leases the shop or office space to various companies. Trying to hook up where a 7-11 is located probably wouldn't be too smart.

Canning

A subject I'm going to touch upon is canning. The reason I say I just want to "touch" upon it is because this topic really deserves a whole article by itself, but since you can use the same tools of the trade, I'm going to mention it here. Cans are those ugly green containers that stick out of the ground. Most of the smaller and isolated cans can be easily opened with vise grips. The bigger ones sometimes have locks on them, but nothing a bolt cutter couldn't handle. Most cans that I've come across come in two flavors: ones where there are just masses of individual telephone wires clumped together, and the others that break apart the clumps of wires to help the distribution of the telephone wires. The ones that have just the bundles of wires clumped together I've found to be of little use. I imagine that a guy would have to match up the two wires for each single phone to get a current that will work. But then again, I'm not an expert.

HARDWIRING PHONE SERVICE

Sometimes these do break up a few individual houses in the neighborhood. There might be a metal plate attached to the top of the can with four or five terminals sticking out. Use trial and error again to find a live current. It is usually pretty easy. The other cans, the bigger ones which are sometimes locked, can be a goldmine. They usually distribute pairs of wires in a horizontal fashion, with a row of metal stubs sticking out. Inside it might look a bit confusing. Around the perimeter, there are wads of wires tangled together and going every which way. Inside the perimeter are rows and rows of square metallic stubs. These stubs are thin, about three eighths of an inch wide, and they stick out about an inch. The telephone wires will connect to both sides of the horizontal rows of these metallic stubs. All you need to do is connect up to two horizontal stubs. Not all of the wires in the can may be live, so you need more than one try. Sometimes these bigger cans have some goodies in them, such as lineman's headsets and papers containing technical data. From what I understand, the purpose of these cans is to help troubleshoot problems by breaking up units (or clusters of wires) into smaller units. I want to emphasize that I am not an expert on these cans. These are just my observations and I'm sure things work differently in different parts of the nation.

The real benefit of hooking up comes when you own a portable computer with a modem. If you find a target computer that you'd like to get to know better, and you're not stupid enough to try to get to it from your home phone, then this might be a good way to go. Portables are going down in price; I've seen some in pawn shops for about $125.

There are a couple of other observations that I'd like to make. I've attended two different high schools and I found their long distance dialing procedures in the same place. On the principal's desk, there was a bread board that slid out on the left hand side. The instructions for making long distance calls were typed on a piece of paper taped to this location. Perhaps this is a common occurrence. I've also lived in a few different dorms, and I've noticed similarities in their setup too. In each room there was a plated telephone jack. The plate was only held down by two flathead screws. I unscrewed the plate and behind were most of the telephone wires for the whole floor. I could have hooked up to any room on the floor undetected.

Finally, if you find that any of the above works out pretty good for you, don't be too greedy, stupid, or start taking life for granted. As they say on Wall Street: "Bulls make money, bears make money, pigs get slaughtered."

BOOK REVIEW

Tune In On Telephone Calls
by Tom Kneitel
Published by CRB Research, Box 56, Commack NY 11725
160 pages, $12.95

Reviewed by Lou Scannon

Telephone calls have been carried on radio waves for years -- from ships at sea, from cars, and, since the advent of microwave and satellite technology, even the average long distance call travels through the ether for a portion of its route. And unlike the private medium of telephone wires, where a physical intrusion is required to listen in on the conversations, radio waves are everywhere around us and need only the right kind of receiver to pull them in.

Although most people know about the existence of car phones, there are a good number of other telephone services on the air: including cordless phones, local marine telephones, ships on the high seas and more. The conversations can range from the ordinary chitchat and gossip of your neighbors, to a lonely seaman talking to his wife or children, or to your local drug dealer planning his next purchase of controlled substances.

Alas, thanks to a recent act of Congress called the "Electronic Communications Privacy Act" (ECPA for short), listening to some kinds of telephone calls over the radio is illegal. Which kinds? Well, it's hard to say. If it's from a car, then it's definitely illegal to eavesdrop, if it's from a cordless telephone, then it's maybe illegal, and if it's from a boat or airplane, then it's perfectly OK. The law does not specify how the radio enthusiast is supposed to be able to distinguish between protected traffic and unprotected traffic.

Fortunately, the Justice Department has announced that they have no plans to enforce this portion of the ECPA which is just as well, as the thought of the Feds breaking into your house to see where you have been tuning your radio tends to put a damper on radiotelephone eavesdropping.

From the editor of *Popular Communications* magazine comes a book that promises to explain how you can become a radio voyeur and listen in. And indeed it does, except by the time you come to the end of the book you're wondering what you paid for. More than a third of the book (60 pages) is composed of channel allocation charts of questionable value. There's no index or bibliography, the latter which would have been useful as the reader is referred to other books whenever the author declines to delve too deep into the technicalities. All in all, a steep price for a few frequency charts and a lot of folksy diatribe against the ECPA. Kneitel may have gotten too used to writing monthly magazine editorials and seems unable to talk about cellular phones without sniping at the industry lobbyists and members of Congress who sponsored the ECPA. Although the ECPA is without a doubt bad legislation that fails to understand the technology it purports to regulate, Kneitel spends far too much space in an already sparse tome whining about it.

For the complete novice, there's a short chapter on what kind of equipment you'll need (a scanner that covers the 870-896 Mhz cellular band and a general coverage shortwave receiver), and a few tips on antennas. Kneitel has a few good words for the Radio Shack PRO-2004 scanner, which after a quick modification (also described in the book) becomes an efficient machine for following cellular calls.

The book covers each portion of the radio spectrum that contains something to do with telephone calls. Car phones, cordless phones, wilderness and remote area phones, radio common carriers, beepers, local marine, regional marine, high seas marine, and oil rigs.

Satellite and microwave links are briefly touched upon, but the equipment needed for intercepting microwave links isn't described. A little miscellany that might not be easily found elsewhere is also included, such as telephone company maintenance frequencies, experimental air and railroad phone services, and the MARS military network used for patching phone calls for uniformed personnel on ships or at U.S. bases overseas.

Although the book is informative, it is a skinny volume at a fat price. With a little trimming, it would have made a good article in *Popular Communications*, and would only have cost $2.50 at the newsstand. For more complete information on channel allocations, Radio Shack sells the "Police Call Radio Guide", which contains complete scanner frequency listings for a particular area. This will tell you just about everything, though it's in a hard to digest format and you'll have to dig for what you want. For station listings in the shortwave band, which will include a worldwide rundown of the maritime telephone frequencies and military MARS frequencies (but again they'll be buried among a lot of other frequency listings), see the "Confidential Frequency List", from Gilfer Shortwave (800-GILFER-1 or 201-391-7887, Box 239, 52 Park Avenue, Park Ridge, NJ 07656.

2600 meetings

First Friday of the month in the lobby of the Citicorp Center, 53rd Street, between 3rd and Lexington, NYC from 5pm to 8pm. Call (516) 751-2600 for more info.

IMPORTANT NOTICE

Rising costs are forcing us to raise our subscription prices slightly. If you renew your subscription before March 1st, you can beat the increase. The old rates are to the left and the new ones are to the right. You can renew now even if your subscription doesn't expire for a long time. We'll just add the time on. You have the choice of tearing out this page and sending it back to us (your address label on the back tells us who you are) or sending one of your own pieces of paper explaining just what it is you want. Please note that even though it obviously isn't the fourth quarter of 1988, this is the Winter 1988 edition and not the Spring 1989 one. We're sorry for any confusion.

☎

INDIVIDUAL SUBSCRIPTION

□ 1 year/$15/$18 □ 2 years/$28/$33 □ 3 years/$41/$48

CORPORATE SUBSCRIPTION

□ 1 year/$40/$45 □ 2 years/$75/$85 □ 3 years/$110/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$25/$30 □ 1 year, corporate/$55/$65

LIFETIME SUBSCRIPTION

□ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date and the same old price!)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25

□ 1988/$25

TOTAL AMOUNT ENCLOSED:

CONTENTS

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

WHEN WAS YOUR
LAST EYE EXAM

Forwarding and Address Correction Requested