2600 HANG UP AUGUST, 1986

VOLUME THREE, NUMBER EIGHT $2

KNOWING UNIX

by The Kid & Co.

The UNIX operating system is popular among most major universities and companies such as AT&T. Learning how to hack and use UNIX is important to any serious phone phreak or hacker.

UNIX is a marvelous system which exists in many different forms: UNIX Release 7, UNIX 4.2BSD, UNIX System V. Currently, efforts are underway to make all systems conform to the UNIX System V interface standards. This will make the jobs of programming Unix systems and hacking them much easier since everything will be "compatible." The techniques I am about to discuss should work under the two most popular versions—UNIX System V and UNIX 4.2BSD. The UNIX operating system has a reputation of not being very secure, yet many attempts have been made to make it that way. Many of them have been successful. Now let us embark on our quest for root (super user privileges).

In order to hack a UNIX system, you must learn how to identify one. UNIX systems all have the same login and password prompts. These prompts appear to be unique to this system, therefore it is not even necessary to penetrate the system to identify it. The login prompts shown below are the standard prompts:

```
login:
Password:
```

In order to start hacking, one must first get into a regular user's account on the system. On some systems passwords are not even required, but they are suggested. Usually there are a few accounts on every machine with no password to them. All that must be obtained to gain entry to these password-less accounts is the username. Finding a username is not an easy thing to do. The system could make the task of finding a username easier if it allowed "command logins." One system I know of allowed anyone to type the username "who" at the login prompt and receive a list of all the users currently logged into the system. If a hacker were to encounter a system with this feature (hole), his job would be made considerably easier. He could collect a list of usernames by using this "who" login several times. Once one has a list of users, all one needs to do is guess the passwords which are typically easy even for the beginner. Here are some usernames along with some likely passwords. Notice the obvious patterns here. The specific usernames are not significant except in the case of root and field since these two accounts appear on every UNIX system.

Username	Password	Comments
root	superusr	The Super User Account
field	hardware	Field Maintenance (has root privs)
ght	gthgth	Average user (notice the pattern)
len	len123	Another average user

Successful login to a UNIX system would look something like the following:

```
login:hacker
Password:
Last login: Tue May 20 23:30:32 on ttyS2

    Welcome to hackvax
    Vax 11/780
    4.2BSD
  * type "man xxxx" for information on xxxx...
$
```

The $ is the command prompt. Once you have this, you are ready to start hacking away. First we will learn how to use the telnet program to send mail to anyone on the system without having your hacked account's username attached to it! You can even make the mail look like it came from *anyone* on the system or even from another system! Below we see a C program which allows you to do this in a nice neat way:

```
#include (stdio.h)  [use 'greater than, less than' brackets on this line instead of parentheses]
main(argc,argv)
char *argv[];
int argc;
(  [use an open squiggly bracket here]
   FILE *popen(), *fp;
   char ch, to[81], from[81], subject[81];

   if(argc != 2)
   (  [use an open squiggly bracket here]
      printf("To: ");
      gets(to);
   )  [use a closed squiggly bracket here]
   else
      strcpy(to, argv[1]);
   printf("From: ");
   gets(from);
   printf("Subject: ");
   gets(subject);
   fp=popen("telnet hubcap 25 ))/dev/null","w");  [use two 'greater than' signs before the '/dev']
   fprintf(fp,"mail from: %s/n",from);  [replace slashes with backslashes]
   fprintf(fp,"rcpt to: %s/n", to);  [same as above]
   fprintf(fp,"data/nSubject: %s/n/n",subject);  [same as above]
   while((ch=getchar()) != EOF)  [use two 'less than' signs after the 'while']
      fputc(ch,fp);
   fputs("/n./nquit/n",fp);  [replace slashes with backslashes]
   pclose(fp);
)  [use a closed squiggly bracket here]
```

This program should be placed into a file which ends in .c on the system and then compiled. One should use either ed or vi to create the file. It is not necessary to explain how to use these programs since that information can be obtained by typing either "man ed" or "man vi" at the command prompt. If we were to place this program into the file fakemail.c then we would use the following command to compile it:

```
cc -o fakemail fakemail.c
```

To run the program, just type fakemail and it will run and prompt you. To terminate the message just type a control-D (the UNIX EOF mark). You can have a lot of fun confusing users by sending mail which appears to be from someone of importance like "root" or other important users.

All UNIX operating systems allow all users to look at the password file. Unfortunately the passwords are all encrypted. One can look at this file by typing "cat /etc/passwd" from the $ prompt. Although you cannot get the actual passwords from this file you can get a list of every user on the system and a list of those users which do not have any passwords. If a user does not have a password, the encrypted password field will be null. The

(continued on page 3-64)

A Trip To England

by John Drake

The following article comes to us from a writer who is spending some time in the United Kingdom. We welcome future contributions from other writers in other countries. Please contact us if you have something to offer.

Phone Card Phones

British Telecom is trying to increase the number of these telephone booths throughout England since there is no money involved, and thus no reason to break into them. Phone cards are the same size as credit cards but they are green on black plastic base. The units of each card are divided up into two tracks of 100 units. Cards come in denominations of 10, 20, 50, 100, and 200 units. One unit is the same as 10 pence. To use the other track on the card (if there is one) you simply turn it around and insert the opposite long length of the card into the phone when the first track is all used up.

The phone "burns off" a unit at a timed interval which is determined by the number you dialed. You can make international calls from these phones. Free calls locally, long-distance, or international can be made from these phones by disconnecting (cutting the wire or inserting a switch) the right wire that contains the incoming timing signals. The wires are color coded but BT (British Telecom) constantly changes this color coding. You can use a voltmeter to deduce which wire you have to cut. The problem arises that the wire is usually hidden and protected unless it's in a school or in a building as opposed to a phone booth. You can always disconnect it at its source which is inside the phone. It stands to reason that since the phonecard phones contain no money that the locks will be lax or, easier yet, standardized for all phones. Once inside, you can disconnect the wire going into the write head.

There is such a phone at an international school in London. The wires of the phone are very bare and I believe that someone at the school has figured out which is the right wire to cut. The students have been making free international phone calls around the world for several months now. British Telecom has been around to fix the phone several times to no avail. Finally, two weeks ago, they cut all the wires and left the phone for dead. During the past week they have reconnected the phone and for the time being it is burning off the credits when you make a call. The wires going into the phone are still bare....

Modem Standards

Prestel's odd standard of 1200/75 has carried over to most other non-Prestel systems. This includes mainframes, Viewdata, and even some BBS's. 300/300 (not U.S. compatible) modems are becoming more popular as are 1200/1200 (U.S. compatible). Other speed configurations are 1200/75 Viewdata and 1200 Spectrum. There is a device which clips onto the modem port and that acts as a buffer for your 1200 baud modem and makes it compatible with the 1200/75 computers here.

U.K. Operator Numbers

999 Emergencies—fire, police, ambulance, cave rescue, coast guard, and mountain rescue
142 Information for London Postal Area
192 Information for numbers outside London
100 Operator Services—alarm calls, advice of duration & charge, credit card calls, fixed time calls, free fone calls, personal calls, international calls, transferred charge calls, subscriber controlled transfer
151 Faults—repair service
193 International Telegrams—send to most countries
100 Maritime Services—ships' telegram service, ships' telephone service
155 Inmarsat Satellite Service
190 Telemessage—if you have something to say and prefer to say it in writing
191 Any other call enquiries

London General Information Services—Charged
(London area code is 01 inside U.K.)

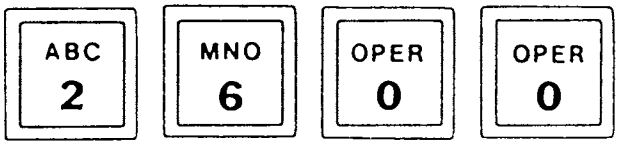
246 8071 British Gas Recipeline (Mon-Fri 8am-6pm)
246 8024 Capital Radioline
246 8050 Challengeline—brain teasers (answer the following day)
246 8007 Children's London—events and competitions
154 Daily Express Cricketline (during test matches played in London and other matches 8am-7pm)
246 8070 Daily Mirror Telefun show
246 8066 Eventline—Motor sport info
246 8026 Financial Times Cityline—for business news and FT index
246 8066 Financial Times Cityline—international market reports
246 8044 Golden Hitline—hits from 60's & 70's
246 8041 Leisureline—daily selection of events in and around London
246 8043 French version of above
246 8045 German version of above
246 8033 National Summaries—Air
246 8030 National Summaries—Rail (Inter City & London Service)
246 8031 National Summaries—Road (Motorways)
246 8032 National Summaries—Sea
246 8000 Puffin Storyline (bedtime stories from 6pm each night)
246 8055 Spaceline (space mission information)
246 8020 Sportsline—general roundup
246 8000 Starline—for your daily horoscope (6am-6pm daily)
123 Timeline—for the speaking clock (24 hour service)
246 8091 Weatherline—London area
246 8008 Woolworth—a selected LP featured each week
160 Woolworth—24 hours a day
168 William Hill Raceline—horse racing results and information

Engineers' Tests

170 to 179 plus your last four digits is the self test number for your phone.
175 Line fault test—Dial 175 then your last four digits, let it ring, you will hear something, hang up. Your phone will ring, answer it, and then dial 9. A list of diagnostics will be read off to you by a computer.

Long Distance Operators

0800 890011 UK to AT&T long distance operators
1 800 445 5667 AT&T to British Telecom's operators



Phone Fraud in Governor's House

Philadelphia Inquirer

Though his aides insist it was mostly a case of "kids being kids," Governor Thornburgh's state telephone credit card was used for hundreds of personal calls, some of them made by members of the governor's family.

The personal long distance calls—dating to the beginning of the Thornburgh administration—were included in bills submitted to the state. They were routinely processed and paid in full. It was only recently, when word of inquiries from a reporter filtered back to Thornburgh's press office, that a review was done on the phone bills.

The review showed that about $4,330 worth of personal long-distance phone calls had been made in a 6½ year period ending in October 1985. All of those calls had been made using the state telephone credit-card number assigned to the governor.

A spokesman said that Thornburgh personally reimbursed the state for $1,751.98 worth of calls made by members of his family. He said the state also had been reimbursed by a private citizen, whom he would not name, for an additional $2,582.52 in personal long-distancee calls that had been made by "a teenager" using the governor's card number.

BB Watching VDT Operators

USA Today

8.6 million video display terminal operators are being monitored by their computers, according to the National Institute of Occupational Safety and Health.

Employers—such as insurance companies, airlines, supermarkets, post offices, and telephone companies—are using computers to record when an operator is off a VDT, count keystrokes by the second, time customer service transactions, and track errors. They say workers do more when they know they're being watched.

"Yes, in the short term you can squeeze more out of people," says Harley Shaiken, technology professor at the University of California in San Diego. "But in the long term, it destroys creativity and the initiative and desire to do a good job."

PSA Inc. of San Diego began in March to give demerits to reservation agents who don't meet certain standards. PSA agents are allowed to leave their terminals a total of 72 minutes during an 8.5-hour shift. They can't spend more than 109 seconds per call and more than 11 seconds between calls. If they do, they collect demerits; 37 in a year could get them fired.

Workers are fighting back in unusual ways. Some are hanging up on customers to reduce average call times. Others fake work, holding a finger on a key and filling computer screens with one letter.

[Readers: we welcome any other suggestions for beating this horrible, nasty system. These people need our help!]

LD Companies Strike Back

The Wall Street Journal

Victor and Betty Humphrey got a surprise package on their 38th wedding anniversary last month; a $258,000 bill for long distance phone calls they didn't make.

GTE Sprint says the 5,600-page, 24-pound bill resulted from fraud. During a six-day dialing spree, it says, inmates at prisons across the country charged 46,000 calls to the Humphrey's code before the company cancelled and replaced the number.

But while the Humphrey's are off the hook, Sprint isn't. They must pay the costs of providing service, whether or not they themselves get paid. Investigators say that illegitimate use of billing codes issued to customers of companies other than AT&T was responsible for a significant portion of the estimated $500 million that the long distance industry lost to toll fraud last year.

The companies are fighting back. Among other steps, they have fitted their switching equipment with anti-fraud software and forged a new industry coalition to bolster prosecution efforts. Some companies permit customers who are traveling to place calls only to numbers in their home area codes.

Many companies have joined the Communications Fraud Control Association, a trade group formed last year to combat toll fraud. The companies complain, however, that they don't always get the cooperation they expect from local law-enforcement agencies.

In February, Teltec Saving Communications Co., a Miami-based long distance company, filed suit in state court against 38 people, including the operators of seven electronic bulletin boards, accusing them of either using fraudulently obtained codes or permitting them to be posted. Although the case hasn't yet gone to trial, some defendants have settled out of court, agreeing as part of the settlement to post the word on underground electronic networks that computer crime doesn't pay.

Teltec has put its own message in bulletin boards where it found its codes posted, offering up to $10,000 for information on who was posting the codes. It has also posted phony codes, then traced people who used them.

Leave Our Poles Alone!

Jersey Journal

In full view of local police, Republican congressional candidate Albio Sires recently carried out his planned "civil disobedience" by nailing a political poster to a utility pole.

"Those are our poles," said a spokesman for New Jersey Bell. "The posters are a safety hazard. We don't want them. We say please leave our poles alone."

Phone Booths Mauled Then Stolen

Long Island Newsday

"Someone apparently used a chain attached to a truck," said a New York Telephone spokesman when he referred to two phone booths that were stolen. Each of the missing booths weighed 400 pounds. And each was secured by a six-inch bolt to a concrete slab outside Weir's Delicatessen in Medford.

Town highway department workers reported the booths missing at 4:50 am. Telephone company employees inspected the site and found only the bolts surrounded by pieces of broken glass as well as smashed panels and rubber molding.

According to Weir's clerk the theft was the final indignity suffered by the booths. "People would slam the phone down, break the receiver, take a hammer and bam," he said. "They'd get mad when they'd lose their money."

The New York Telephone spokesman said that public phones get "bombed, bludgeoned and stuffed." But, he added, "It's unusual to see a booth hauled off."

New York Telephone is offering a $2,000 reward for information about the theft. The number to call is 8005225599. The numbers of the missing payphones were 5167328600 and 5167328550.

The Ghost in the Machine

Time

The 911 operators have learned that when they get a call and hear no voice on the line, a cordless phone is frequently at fault.

A rogue phone's dialing system is apparently triggered by low batteries, or by interference from household gadgets such as microwave ovens, fluorescent lights, hair dryers, and garage-door openers. Three-digit numbers are hit most often (411 for directory assistance also gets such calls).

For emergency operators, the problem is more than a nuisance. Silent calls must be traced, in case a human rather than a phantom needs help.

letters of the month

Dear *2600*:

Congratulations on the apparent success of your newsletter. I learn something from each issue. Your points on the power of computers and the information that is processed on them are correct. And you provide a valuable service by attempting to educate your readers and (sometimes) chide those who would use the information improperly.

I work on the other side of the fence—data security for a large corporation. I don't always like what you say about the condition of my profession—because it is usually too painfully true!!! I also have the nature to try, test, and explore new areas to see what happens. But I wouldn't proceed to the point of "crashing" or "disabling" a system as was stated on page 3-42 of your June issue. Finally, the point of my letter!

Please don't tell people how to crash a computer system. It may prove your technical superiority, or that you can read a technical manual. However, just as the lives of many innocent people connected with your BBS and others were unjustly and adversely affected by raids by uneducated and unqualified intruders, crashing a major (or minor) computer system has serious consequences to innocent people, directly or indirectly. And, unless you know the effect you have on my business (retail, oil, banking, public utility, medical care, etc.), you are just as naive, over-your-head, and dangerous as the authorities that confiscate a BBS.

On a lighter note, we don't need your help anyway. We crash our systems on an irregular basis. Unintentionally, of course. Which helps explain why you see so few computer professionals loitering in pool halls these days. They are too busy trying to recover from the latest/greatest technology.

Keep up the good work.

The Stopper

Dear Stopper:

Please note that those people who confiscate BBS's get the full support of law, unlike those who crash main-frames.

On whether or not we will stop printing system shut-down procedures...that is something we shall consider. Our main point is to show how easily it can be done by anyone—a computer buff or a saboteur.

Dear *2600*:

I am a lawyer with an avid interest in BBS's or SIG's that handle law-related material or are aimed at lawyers. Do you or your readers know of any such boards other than the SIG's on CompuServe, the Source, and Bix? Are there any that have shut down? I would like to hear from anyone who has had any experience with these boards or lawyers who use them.

I am on CompuServe, BIX, and ABA/net (1825).

Rees Morrison
14 Montrose Road
Scarsdale, NY 10583

Dear Mr. Morrison:

Please send us the list of the law-related BBS's that you know of, and we ask our other readers to do the same. We can publish them in the near future.

Dear *2600*:

As a veteran VAX/VMS wizard and a new subscriber to *2600*, I was interested to see the front-page article (July 1986) on the subject of VMS security hacking. I was disappointed, though, to find that "Violating a VAX" dealt with the subject at a junior-high level. I'm not necessarily criticizing the article or its author on that account; we all have to crawl before we learn to walk, and all that. However, I'd like to save would-be VMS hackers some embarrassment by pointing out a few mistakes to avoid. If you do things Baalzebub's way, your friendly local system manager will soon be knocking at your door with a sheaf of printouts in his hand and a stern look on his face.

The password-grabber command procedure presented in the article illustrates a number of blunders:

1. First, that "%DCL-F-TRANS" crap is completely bogus, in several senses of the word. Why bother faking a login and making up an error message when you can just simulate a user validation error and make it look as though the user has mistyped his password? Simulating a login error and killing the process is a lot safer than presenting the user (who may not be all that stupid, even if he is a system manager) with a series of obviously bogus "system" messages.

2. You can use the DCL command "STOP/IDENT=0" to log out without generating a message. This doesn't require any privilege at all. In a program, you can use SYS$DELPRC.

3. Using INQUIRE to read the username and password is foolish when you can use the READ command with the /PROMPT and /ERR qualifiers. Also, READ has a timeout option. By the way, the default timeout count at login is 30 seconds, not 20 seconds as implied in the article.

4. The command procedure given doesn't use SET MESSAGE to get rid of any error messages which might possibly be generated if things go wrong—another potential source of user tip-offs that something fishy is going on.

Where VMS is concerned, the whole password-grabber concept is practically obsolete anyway, since VMS V4 defines a terminal characteristic called "SECURESERVER" which was designed specifically to foil password-grabber programs. When a terminal line has this characteristic set, pressing the BREAK key at login is guaranteed to disconnect any process running on the terminal.

A few other notes: 1) Control-T isn't very useful at login time. Repeated control-Y's immediately following the password are more useful, but the "DISCTLY" flag in the UAF prevents them from having any effect. 2) Using "890" as a file version number is silly. (Suppose that version 891 or higher already exists.) The number you want is 32767; that's the maximum possible version number. RTFM! 3) The first "Trojan horse" procedure given should include the command "SET DEFAULT SYS$LOGIN" before the DELETE command which is supposed to get rid of the incriminating LOGIN.COM file.

As operating systems go, VMS is very secure, and it's becoming more so with each new release. (Unfortunate but true.) According to DEC, a version of VMS will have the Defense Department's highest possible security rating within two or three years.

In parting, I offer you at *2600* a slogan for your masthead: "The road of access leads to the palace of wisdom." Apologies to William Blake.

j

Dear *2600*:

I noticed a problem in the password grabber described on page 3-49 of your July 1986 issue. In the narrative, it says that control-Y is disabled, but the code doesn't actually disable control-Y: it merely provides direction on what to do if a control-Y is encountered. In this case, if a control-Y is entered during the wait period, then the program will just continue with the next step after the control-Y interrupt. Since there is no step after the WAIT, the program will exit in this case. To use the ON CONTROL-Y effectively in this case, you need to loop back so that any control-Y will reset the wait timer: $LOOP:, $ON CONTROL-Y THEN GOTO LOOP, $WAIT 01:00:00.

An even better solution would be to actually disable the control-Y early in the program with a SET NOCONTROL command. In fact, it would be useful to also disable control-T

(continued on page 3-64)

The 2600 Information Bureau

10007	Telemarketing	202 783 7213	[DC, Philly, part of VA]
10054	Eastern Telephone	215 628 4111	[Philly]
10066	Lexitel	800 631 4835	
10080	Amtel		
10084	LDS Metromedia Long Distance		
10085	Westel, Inc.		
10203	Cytel		
10211	RCI	800 458 7000	
10220	Western Union		
10221	Telesaver 201 488 4417,	202 982 1169	[eastern cities]
10222	MCI	800 624 6240	
10223	TDX Systems, Inc. (for business only)		
10235	Inteleplex	609 348 0050	[Southern NJ]
10288	AT&T	800 222 0300	
10333	US Telecom	800 531 1985	
10366	American Telco, Inc.		
10444	Allnet	800 982 8888	
10464	Houston Network, Inc.		
10488	ITT	800 526 3000	
10777	GTE Sprint	800 521 4949	
10800	Satelco		
10824	ATC/Directline		
10850	Tollkal	800 646 1676	[Northern NJ]
10855	Network plus	703 352 1171	[DC metro area]
10888	SBS Skyline	800 368 6900, 235 2001	[no auto EA, need acct]

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

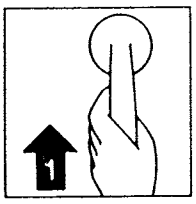
Cartoonist
Dan Holder

Junk Mail Receiver
Richard Petrovich

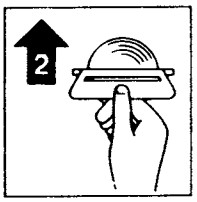
Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600
BACK ISSUES: $2 each, individual; $3 each, corporate. $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork and data for publication.
POSTMASTER: This is private mail

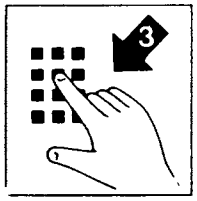
Phonecard



1. Lift the receiver and listen for dial tone (continuous purring or new dial tone – a high pitched hum).



2. Insert the card into the slot, green side up, in the direction of the arrow, and press it fully home.



3. Dial the number you want. The digital display will show the number of unused units on the card (or on the track actually inserted in the case of a 200 unit card). Listen for the ringing tone and speak when connected. The credit units are progressively erased as shown on the digital display.

Follow-on calls.

If you have unused units remaining on a card and you wish to make a new call, do not replace the receiver. Instead, briefly depress and release the receiver rest. As soon as you hear the dial tone again, you can make your next call.

(see page 3-58 for more details on this)

This is a list of area codes and the number of exchanges being used in each one.
It will give an idea of what area codes are filling up, as well as which ones
are unused. This list comes to us from Telecom Digest, via Private Sector.

NPA	COUNT	COMMENTS
201	543	North Jersey. Getting right up there.
202	437	
203	349	
204	308	
205	522	
206	431	
207	306	
208	246	
209	257	
212	467	
213	524	Los Angeles already split off 818.
214	542	A Dallas split is rumored soon.
215	481	
216	477	
217	325	
218	267	
219	307	
301	538	Maryland. Busier than 617.
302	73	Delaware. Every state gets one, y'know.
303	557	Colorado has been growing...
304	298	
305	540	Miami too.
306	416	
307	133	Wyoming.
308	186	
309	237	
312	640	Why hasn't Chicago split yet?
313	504	
314	454	
315	228	
316	332	
317	325	
318	298	
319	308	
401	108	Rhode Island.
402	385	
403	544	Alberta and some NWT - Canada's busiest
404	456	
405	462	
406	316	
407	0	
408	216	
409	255	
410	0	
412	377	
413	109	W. Mass - what a waste of a good code!
414	378	
415	483	San Francisco, also rumored for split.
416	433	
417	181	
418	327	
419	304	
501	480	
502	310	
503	441	
504	267	
505	261	
506	143	
507	249	
508	0	
509	213	
512	501	San Antonio, TX.
513	396	
514	363	
515	377	
516	283	
517	285	
518	211	
519	286	
601	358	
602	440	
603	193	
604	480	
605	310	
606	240	
607	146	
608	210	
609	204	
610	0	
612	424	
613	220	
614	338	
615	430	
616	317	
617	533	E. Mass - splitting off 508 in 1988
618	300	
619	329	
701	333	
702	195	
703	415	
704	265	
705	239	
706	96	Northwest Mexico hack, not a real NPA
707	145	
708	0	
709	237	
710	0	Unlisted code used for AT&T Government services.
712	265	
713	414	
714	364	
715	288	
716	322	
717	410	
718	294	
719	0	
801	265	
802	167	
803	396	
804	371	
805	193	
806	225	
807	97	W. Ontario - another waste.
808	163	
809	340	
810	0	
812	243	
813	344	
814	237	
815	255	
816	401	
817	381	
818	240	
819	282	
900	24	
901	178	
902	221	
903	0	
904	356	
905	206	
906	109	Upper Michigan, tied with 413.
907	340	
908	0	
909	0	
910	0	
912	270	
913	399	
914	256	
915	257	
916	319	
917	0	
918	257	
919	510	North Carolina's growing quickly.

SYSTEMATICALLY SPEAKING

USSR Computer Hungry

Long Island Newsday

The Soviet Union has announced sweeping reforms in its "obsolete" higher education system, which it said produces doctors who cannot diagnose and engineers who know little about computers.

"Materials and techniques are obsolete. That is why there is a need for the profound restructuring of higher and secondary specialized education," the Communist Party newspaper *Pravda* said in announcing proposed changes that will affect 2 million students and set up thousands of computer-equipped workplaces to make Russians "computer literate".

ATM's in China!

Combined News Sources

NCR Corporation has installed the first automatic teller machine in China. The unit will be operated as a test case by the Nantung Bank in Zhuhai, an economic "free zone" near the Hong Kong border. The machine won't be available to citizens of the People's Republic.

Cash Machines Are Popular

New York Newsday

Just a year after the New York Cash Exchange was formed, the system that lets customers of one bank use automatic tellers at competing banks has virtually run out of institutions to recruit.

The regional system now has 1,225 machines and 4.2 million customers, making it one of the largest in the nation. The 55 institutions set to join will boost NYCE to 2,000 machines and 6.5 million customers, with a total of 80 institutions in eight states, the District of Columbia, and Puerto Rico.

The system's chief New York rival is Citibank, which has its own network of 626 machines and 1.5 million card-holders. Citibank has shown little interest in joining NYCE.

NYCE may try out a new project—a debit-card system. If such a system were in place, a customer could buy clothing at a local department store using a bank card, and a sales clerk could deduct the purchase price right from the customer's checking account.

TV Blue Boxes

Radio Electronics

The coming generation of digital TV sets is designed for easy servicing by reprogramming them. Access for servicing, in the case of sets using ITT digital IC's, is provided via a rear-panel connector or by dialing up a special code on the wireless remote-control unit. In both cases, that gives the repair technician access to the set's control bus. From there, it would be an easy matter to defeat the sync-suppression decoding used by most cable-TV systems for their premium channels, according to engineers of the National Cable TV Association. The NCTA fears that the introduction of digital TV sets will lead to a flood of "blue boxes" to let cable subscribers decode pay-TV programs without paying for them. The NCTA has written to all major TV set manufacturers urging them to "take the necessary steps to make it impossible to externally force" one of ITT's VLSI chips to defeat pay-TV encoding.

New Chip Helps Sprint

USA Today

About 30 percent of telephone customers won't get equal access service until 1987 or later. Those customers would ordinarily be lost to US Sprint, because to get on Sprint's system the customer would have to dial more than 20 digits. So Sprint came up with a microprocessor that automatically dials all the Sprint access numbers when a user dials "1." Sprint will install it free on the premises of any customer with bills of $150 or more.

Government Phone Fate?

The New York Times

The Federal government has started to update its entire system of lines, switching equipment, satellites and security devices, which has been in place since 1964. The current system is still managed by AT&T and cannot handle the demand of increased numbers of calls and high-speed data communications.

The General Services Administration has invited communications companies to come up with ideas for a new system. The Government's next phone company, like AT&T, will be privy to information about encoded data and will therefore be required to have a high-level security clearance. The companies are being asked to devise advanced ways to protect communications from phone tapping, sabotage, and even disruption caused by the electro-magnetic pulse that destroys conductors of electricity after a nuclear explosion.

The system, "FTS 2000", is expected to be in place by the year 1990 and will cost 4 billion of your tax dollars.

Rural Radio Phones

Communications Week

Four telephone associations and the Rural Electrification Administration (REA) have asked the FCC to set aside certain radio frequencies to be used for telephone service in rural areas.

Using radio instead of land-based wire could lower costs of connecting customers, permitting telcos to extend coverage in areas where costs have previously prevented it, according to the group's FCC filing.

They called the radio service Basic Exchange Telecommunications Radio (BETR).

If the request is granted in full, BETR could extend service to an estimated 485,000 customers nationwide who are currently without telephones. Another 400,000 could have service upgraded from multi-party to one-party lines.

The groups want the FCC to allocate 26 channels in the 450 MHz band and two 800 MHz channels to BETR.

"Debugging" Phones

Business Week

It may not be what the phone company had in mind when it came up with the memorable slogan "Reach out and touch someone," but a tiny company called BioHygenix Inc. plans to publicize a list of unsavory bacteria and fungi that it says inhabit the mouth and earpieces of most telephones.

The Fremont (CA) startup, of course, is providing more than a public service. It has a product: a patented plastic telephone cover impregnated with vinyzene, an antimicrobial preparation developed by Morton Thiokol Inc.

UNIX

(continued from page 3-57)

format of /etc/passwd entries follows:

user:encrypted pwd:user #:group #:misc. info:home dir:prog executed upon login

Examples from an actual /etc/passwd file (the first 4 accounts are present on virtually all UNIX systems):

```
root:QtmvlCL0bmtbg:0:10:System Account:/:/bin/csh
daemon:*:1:31:The devil himself:/:
uucp:xxx:4:1:UNIX-to-UNIX Copy:/usr/spool/uucppublic:/usr/lib/uucp/uucico
field:ivzH0hALU.aGo:0:10:Field service account:/usr/field:/bin/csh
paul:VkFuS77wLi0gM:5:10:Paul G. Estev:/usr/users/paul:
lenny::10:20:Lenny Kern (dumb user w/no passwd):/usr/users/lenny:/bin/sh
```

Those entries in the password file which have a user number of 0 are accounts which have super user privileges and should be primary targets for password hacking techniques.

This should be enough to get you going on UNIX hacking. Look for part two which will contain more advanced methods of hacking.

letters

(continued from page 3-60)

while the Password Grabber is running; that would avoid the situation described in the second paragraph of the article. For example, if the victim has the presence of mind to enter a control-T while the password grabber is at the WAIT step, it will be obvious to the victim that he is still logged on. The solution is to enter SET NOCONTROL=(Y,T) early in the program.

Stake Out

Dear Readers:

Last month, you read about the "free phones of philly." Chester Holmes told you about free calls from various payphones that have equal access.

One of our writers was on a recent trip across the country, and he had an opportunity to test Mr. Holmes' discovery out in other cities around the nation.

In Chicago and Los Angeles, for example, pay phone calls are free when one simply chooses an alternate carrier before dialing. 10444, 10777, and 10888 worked. A more complete list (furnished by Kid & Co.) can be found in this month's 2600 *Information Bureau.*

For you Telco executives—you should realize that Philadelphia, Chicago, and Los Angeles are among the largest cities in this country and represent a very large hole to patch (not to mention the rest of the free world).