There is a very simple method of getting accounts and passwords called a simulation. What you do is imitate the operating system, so that when an unsuspecting hacker comes up and sits down, he types in "ENTER USERID" or whatever, he types it in the program, the program records them in a file, and you have a new account.

The skill comes in here. You have to make your program simulate the operating system very closely, so that no one can tell that they are in your program, not the OS. You must make your program give all the appropriate error messages if the guy makes a typo, or if he tries to enter an OS command, or if he presses the break key (if your system uses break), or slips in some control characters. There are other ways some might think that he is not really in the OS, so try to anticipate all of them. Most likely he will think the computer is just spacing out, and forget about it. But you might get a system programmer who will know what you are doing immediately.

Also, when you collect some guy (how come there are very few passwords), you don't want him to know that you just got it, or he'll just go and have it changed. So, there is a trick called slipping back into the OS. If you are on a paper printer (TTY or whatever) you may have to slip out of the OS too. What it is, is this. You're program is supposed to imitate the OS so that no one call tell they're not in the OS. Now when you start your program, it has to look as if you never left the OS. This sounds hard to do, but again there is a trick. You start your program, and then you let it pretend whatever you want your system prints when a program ends. Now it looks like your program has just finished, but it didn't really. Also, it is wise to have your program print some junk pretenders, so that no one call tell they're not in the OS.

Now you have your program running, but it looks like the OS. So the next step is to pretend to log out. You type in "BYE" or whatever for your system, and have the program return whatever bullshit it prints when you log out. Then you leave. Don't stick around after this, you'll just look suspicious.

Now some hacker comes up and types whatever your system needs to give. "ENTER USERCODE". (What if he doesn't type it right? Don't let your program ask for the usercode unless it is correct, after all, the OS wouldn't.) You collect his account number and password, and enter them into a data file, which you will come back and print up later. That's the simple part.

Now comes the hard part. The guy just logged onto his account, or he thinks he did. You can't imitate the entire system, in fact don't want him to think he's even on his account, because imitating his account is a hell of a lot of work (I tried once). So, bump him off with an error, about how his password is wrong whatever. Now he knows his password is right he used it yesterday or whenever, but he'll think he made a typo. Once, maybe twice. After that, he'll go get help, and the system will discover what he did pretty quickly, so you can't give him reason to go for help.

After you get his password and give some error, you have to let your program slip back into the real OS without letting him know, so that he can type it in again and really get into his account. This part is the hard part. There is usually some way for a program to log out on its own in every system, look it up in the manuals and have your program log out. The problem here is that you will log like a log out, and there is no legit reason why the system would print a log out message at this point. You can either try to cover up the log out message, or print some bullshit to explain it, or there may even be a way to suppress it. Every system is different. I can't give any specifics on this.

Then you come back later and print up his account and password! This method will work. I have used a simulator on several systems, and I have always gotten good results. There are many other methods for breaking into computers, but most are specific for some particular system. If you have any other ideas, send them in!

Also, if anyone needs specific data on any aspect of a Hewlett-Packard 2000 system, especially the 2000/ACCESS model, send a SASE to TAP to be forwarded to me, and I can probably tell you whatever you want. I worked for several years as a systems programmer/system operator on one, and I know almost everything about it.

For all of you TAPPers into Sci-Fi and computer hacking, there is a fantastic book called "The Adolescence of P-Iry" by P-Iry. P-Iry is a heuristic computer program, with a tendency to take over the operating systems (OS) of large computers, especially those belonging to the Pentagon. (Ugh! Fuck the registration!)

One more note. If you would be interested in getting a lineman's handset, just find some nice cool phone man, go up, talk to him, ask him about a ringback or two to break the ice, and then ask him if he could kind of lose his handset for a small price. I picked one up from a really cool lineman for five bucks, and I got a Bell hardhat for $2.50. Also, they are glad to talk to you about all kinds of ANI's, test numbers, and such. Just make sure you get a lineman, not a supervisor.

Long live Robert Heinlein! This report from California is brought to you by:

Simon Jester

TAP RAP by TOM EDISON

Some good news and some bad news. First the good news. Starting with this issue, TAP will be published every month. Now the bad news. Due to inflation, printing costs, and the resent outrageous Postal Monopoly rate hikes, TAP must raise all subscription rates. A ten issue one year Bulk subscription will now cost $7. A ten issue one year First Class subscription will now cost $10. For those subscribers who like their issues delivered in a plain unmarked envelope but don't want to pay the new increased First Class rate, I have created a new subscription type which will be bulk mailed in a plain unmarked envelope. This new Bulk Envelope subscription will cost $8. All TAP back issues will be 75 cents each except issue $50 which will be $1.50. All of these new rates go into effect on February 1, 1982.

You can still order new 2000/ACCESS books, and you will now get all of your issues mailed First Class. You will have to prepay for the following news but due to the expense of mailing every month, all previous First Class subscribers will now get their issues mailed Bulk Envelope. If you still want to receive your issues mailed First Class, you will have to send an additional $2. It costs TAP $2.40 to mail out 12 issues and this does not include the cost of the envelopes.
I have heard about a book called the "Radio Engineers Handbook", which contains specs on all sorts of electronic stuff, including phone systems. They have info on frequencies, standard impedances, etc. I don't know who publishes it. Also, the IEEE (Institute of Electrical and Electronic Engineers) and the EIA (Electronic Industries Association) publish handbooks of electrical standards, which includes the same type of stuff. info on normal electronic circuits plus sections on phone line standards. They may be of interest to Tappers, and are probably available at the library of any large university.

I have heard that silver boxes are being used in LA, on an experimental basis only. I believe that they only let you tap into numbers in the area code the system is in. One possibility that I thought of is tapping into data lines. You can record standard 300 baud digital data on a normal cassette tape, and later play it back into your microcomputer. You would probably have to work to locate the machine they are using, and you would have a chance of picking up some account numbers and passwords. Then just dial up the number you are tapping, log in, and the machine is open to you.

There are special computer data lines known as hard wire lines, like direct TW lines I think. Does anyone know if you could use a silver box to tap into a hard wire line? Hard wire lines aren't given regular phone numbers. they have special numbers like (815)747. Do you convert that into a standard number, or can you? Do they run through the same exchanges as normal lines? If not, can you dial into hard wire exchanges? If you could get in, there are many possibilities. Banks, among other people, run data over hard wire lines which they presume to be secure. If you know anything about data lines, please get off your ass and write to me, Simon Jaster, c/o TAP.

Any of you who have apple micros might be interested in getting the apple-cat modes. It is like a normal mode, but has a few very nice features. It can dial numbers and has auto-answer, like most, but besides dialing in pulses it can use touch tone, and it can receive touch tone data. This would allow you to use your computer from any phone without a terminal, by simply using touch tone instead of a normal carrier. Also, it would make it very easy to break into Sprint and the like. The only problem is that the apple-cat costs over $300. Oh well.

Any of you hackers might be interested in two good bulletin board systems (BBS). One is BBS #1 in Santa Clara, CA, at 408-296-5799. It is up 24 hours a day, and uses 110, 150, 300, and 1200 baud. I have never figured out where BBS #2 is. It is hard to get a line because there are so many people trying to use it, so just have patience and call back again. And again. And again. I promise it is not down. Just very very busy. Another BSI at CBBN/RW also up 24 hours. In Portland, OR, at 503-866-5510. They both have phone stuff and mail. I've seen lists of Sprint codes on BBS. Don't put anything too blatantly illegal, because the FBI has been known to log in occasionally and check these systems.

I have heard a rumor from Orange county, CA that sounds very interesting. It seems that they are testing some new system, where when you get a call and pick up your handset, just after the ringing stops and before the battery connects, the number calling is sent to in binary pulses. I don't know if this is true as I don't live near Orange county nor do I know anyone there. But if you live there, check this out. The pulses are supposed to come down in "sideways binary", using a 5 bit word length, the digits represent 0,1,2,3,7 instead of the usual 0,1,2,3,4. This is so that there are never more than 2 bits set in any one word since you only go up to 9, not 16. There should be 7 words, and I have no idea what they use as start and stop bits, or if they do. The pulses could be from 3 to 50 ms long.

If anyone in Orange county can detect these pulses, let us know!

As I'm sure you all know, Bell is slowly but surely going to out of band signalling. This means that I will have to throw away my blue box in a few years, and if I had a black box I'd have to dump that too. In fact the only box that may be of any use will be the red box. Fortunately, Sprint and the other alternate calling networks are filling in gap caused by out of band signalling. There are four alternate calling companies, Southern Pacific Communications (sprint), ITT (citcall), MCI, and Western Union. They all offer two plans, one for business in which the code works all the time but costs a lot, one for home in which the code only works at night and on weekends. Sometimes home codes work during business hours but you get charged prime time rate. They all have lousy quality lines, with almost no hiss or clipping compared to alternate companies. In fact some of the alternate companies lines are so bad, that after stealing a code, I was unable to run computer data over it because my modem wouldn't hold a carrier on it. Sprint has the best quality lines, but even those are inferior to Bell long-lines. Also, you often have problems putting a call through, getting a busy signal when the other person phone is on the hook and such. Again Sprint does the best on this, putting through calls more often on the first try. MCI appears to have the next best quality equipment, with ITT and Western Union behind. Much of the problem is because Bell won't give these companies the same quality connections that it gives its own long-lines dept. The quality will continue to go up as equipment is improved and they win more court battles forcing Bell to give them better quality connections on both ends. Another problem is that alternate calling nets don't go everywhere Bell does. Note that I know of go international yet, although Sprint is planning to soon. Sprint goes to the most places in the US, 90 major cities. ITT goes to 105 major cities. MCI to 86 major cities and Western Union to 29.

If you want a list of where each service goes, call their service rep (list in yellow or white pages) and ask. Also ask for info on subscribing, they'll send you a packet with all sorts of goodies in it, like lists of cities they go to and sometimes access numbers. If you want to read a good (but straight)
article on alternate calling nets. Consumer Reports wrote these up in its early 1981 issue, available at any library.

Alternate nets can be just as dangerous as a "call if you caught. They often have automatic traps on all incoming lines, so don't call from home. (No shit!) If you go scanning a bunch of codes, you can be sure that you'll set off a bunch of flags in their office. If you can, try to conceal the number you are calling, because they will try to hassle the person receiving the calls if they can't find out who is making them. Just like Bell. Call your friend through a loop-around, or better yet, call up to the city he lives in, then call the access number for another alternate net, and make a local call on it to your friend. For instance I call from San Diego to San Francisco on JC1, then I have JC1 call Sprint in SP; then I go through Sprint and make a local call in SP. This way JC1 can't find out where I called to, and Sprint isn't going to waste time worrying about a local call.

"Make sure you don't call through another access number of the same sort, because that sets off a red light on a board somewhere in the office, and they will want to know what you are up to. Also they can easily trace the call through their own net no matter where you run it. If you are caught, they may just make you pay for whatever they can get you to. JC1 is known to do that. You could be busted through kickbacks and breaking FCC regulations, both federal crimes. Also in California, there is a law against computer crimes. It is a tough way, and the way it is written, they can bust you for looking at a computer wrong. (The Fucking Legislature)..."

Alternate calling nets are actually just large computer networks, so guess what else the DA will go after. You can't find out where I called to, and Sprint isn't going to waste time worrying about a local call. If you have a micro computer, you can spoof (or even an audio interface to your phone line and program your computer to scan through possible codes. Until it finds a good one. A micro can scan more codes in an hour than you could in a day, and it doesn't make mistakes or get tired. If you don't have a micro yet, you will soon. They are the box of the future, and are quickly becoming the box of the present.

Have TAC Phone Phreaking Simon Jaster

Getting wrong numbers

Futuristic mathematical reasoning is one of the most prevalent and destructive forces for our national health. It has spread like a cancer through the highest offices of the Reagan administration and gobbled much of the recent thinking in the arts and sciences. Perhaps you have heard of the "computers" that have been built in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the next few years.

The Phone Company has been playing several card games recently about the course of crime prevention. Perhaps you have heard about one of the computer-assisted crime prevention project that is going on in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the course of the next few years.

Alternate calling nets are actually just large computer networks, so guess what else the DA will go after. You can't find out where I called to, and Sprint isn't going to waste time worrying about a local call. If you have a micro computer, you can spoof (or even an audio interface to your phone line and program your computer to scan through possible codes. Until it finds a good one. A micro can scan more codes in an hour than you could in a day, and it doesn't make mistakes or get tired. If you don't have a micro yet, you will soon. They are the box of the future, and are quickly becoming the box of the present.

Have TAC Phone Phreaking Simon Jaster

A scheme you can bank on

Grannules, Calif. - A top video game maker has been accused of using a scheme that involves bank customers to make their deposits in a high interest bank. The scheme, known as "The Scheme of the Century," is said to be a major factor in the recent rise in interest rates. The scheme is similar to the one used by the computer-assisted crime prevention project that is going on in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the course of the next few years.

The Phone Company has been playing several card games recently about the course of crime prevention. Perhaps you have heard of the "computers" that have been built in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the course of the next few years. Perhaps you have heard about the computer-assisted crime prevention project that is going on in the course of the next few years.

Alternate calling nets are actually just large computer networks, so guess what else the DA will go after. You can't find out where I called to, and Sprint isn't going to waste time worrying about a local call. If you have a micro computer, you can spoof (or even an audio interface to your phone line and program your computer to scan through possible codes. Until it finds a good one. A micro can scan more codes in an hour than you could in a day, and it doesn't make mistakes or get tired. If you don't have a micro yet, you will soon. They are the box of the future, and are quickly becoming the box of the present.

Have TAC Phone Phreaking Simon Jaster

Classified

Up to 20% MOR. for under $1.00
Amazing but true, a simple device costing cents enables this fantastic gas saving. Easily installed.
What it is, where to get it, how to fit it. confidential report with full information, send $4.00 cash or $5.00 check) Plus SASE to Box # T.

Continental Spectator

EVERYBODY SWINGS WITH "CONTINENTAL SPECTATOR"

...122 full-color pages loaded with personal ads and nude photos
...Highlights: listings—many with addresses & phone numbers
...Sex singles, pretty girls, gay & bi males who want to meet YOU
...Plus intriguing articles, stories, nude photos, 
...lists to meet swingers and MORE
For a copy of the latest mailing list, send $4.00 to CONTINENTAL SPECTATOR, Room 603, Dept. T, New York, NY 10036

NEED: 1) Plans/schematics for scanners.
2) Plans and info. on antenna construction (any band).
3) Copies of material from Information Unlimited, Scientific Systems and Solaser.
4) Info. on the MAC-ML8 (TAP #58) and a replacement for Special Parts Ltd. (defunct).
5) Books and back issues of publications covering electronics, defense and alternative technologies.

I have other plans available and will trade for above or will make other arrangements. SASE to Box L.

---

PICK LOCKS

THE SCIENTIFIC WAY WITH COMPUTER DESIGNED TOOLS ORIGINALLY DEVELOPED FOR ISRAELI INTELLIGENCE

The 1978 catalog of CONFIDENTIAL ELECTRONIC DEVICES is now available at a special introductory price of $5.00. This is the first time this catalog has been offered to the public at this low price. Full information regarding the catalog and how to obtain it is available upon request. For more information or to order the catalog, please contact us at 147 California Street, San Francisco, CA 94109.

---

THE TAP CLASSIFIED AD SHEET IS PUBLISHED AS A SERVICE TO OUR READERS. ALL ADS MUST BE TYPED AND CAMERA READY. ADS WILL APPEAR IN THE NEXT AD SHEET UNLESS THEY ARRIVE AFTER PRINTING DEADLINE IN WHICH CASE THEY WILL APPEAR IN THE FOLLOWING SHEET. THE COST PER ADS PER ISSUE IS $2. IF YOU WISH TO PRESERVE YOUR ANONYMITY, TAP BOX NUMBERS ARE AVAILABLE AT THE COST OF $4 PER AD PER ISSUE. FULL PAGE ADS COST $10 AND HALF-PAGE ADS COST $5. PAYMENT MUST ACCOMPANY ALL ADS. SEND CASH AND GET A 10% DISCOUNT ON ALL ADS. ADDRESS ALL AD REQUESTS TO: TAP, ROOM 603, 147 WEST 42ND STREET, NEW YORK, N.Y. 10036.

---

TAP, ROOM 603, 147 W. 42 ST., NY 10036

---

CONSUMERS REPORTS

P.O. BOX 23, BROOKLYN, NEW YORK 11203

---

HANDLE WITH CARE

TRADEMARK/® 1978

---

THE SCIENTIFIC WAY WITH COMPUTER DESIGNED TOOLS ORIGINALLY DEVELOPED FOR ISRAELI INTELLIGENCE

THE 1978 CATALOG OF CONFIDENTIAL ELECTRONIC DEVICES IS NOW AVAILABLE AT A SPECIAL INTRODUCTORY PRICE OF $5.00. THIS IS THE FIRST TIME THIS CATALOG HAS BEEN OFFERED TO THE PUBLIC AT THIS LOW PRICE. FULL INFORMATION REGARDING THE CATALOG AND HOW TO OBTAIN IT IS AVAILABLE UPON REQUEST. FOR MORE INFORMATION OR TO ORDER THE CATALOG, PLEASE CONTACT US AT 147 CALIFORNIA STREET, SAN FRANCISCO, CA 94109.

---

THE TAP CLASSIFIED AD SHEET IS PUBLISHED AS A SERVICE TO OUR READERS. ALL ADS MUST BE TYPED AND CAMERA READY. ADS WILL APPEAR IN THE NEXT AD SHEET UNLESS THEY ARRIVE AFTER PRINTING DEADLINE IN WHICH CASE THEY WILL APPEAR IN THE FOLLOWING SHEET. THE COST PER ADS PER ISSUE IS $2. IF YOU WISH TO PRESERVE YOUR ANONYMITY, TAP BOX NUMBERS ARE AVAILABLE AT THE COST OF $4 PER AD PER ISSUE. FULL PAGE ADS COST $10 AND HALF-PAGE ADS COST $5. PAYMENT MUST ACCOMPANY ALL ADS. SEND CASH AND GET A 10% DISCOUNT ON ALL ADS. ADDRESS ALL AD REQUESTS TO: TAP, ROOM 603, 147 WEST 42ND STREET, NEW YORK, N.Y. 10036.