TAP

TAP
Room 603
147 W. 42 St.
New York 10036

MA BELL IS A CHEAP MOTHER

JANUARY 1982 No. 71

Simon Jester Issue

I have a little for all you computer phreaks out there. If you have access to a hardwire terminal hooked up to a mini or maxi system, not a micro, and want to collect a few passwords and account numbers belonging to other people, read on.

There is a very simple method of getting accounts and passwords called simulation. What you do is imitate the operating system, so that when an unsuspecting hacker comes up and sits down, the terminal types "ENTER USERID" or whatever, he types it in, it then types "ENTER PASSWORD", he types it in, 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 someone might accidently find out that he's not really in the OS, so try to anticipate all of them. Most likely he will think the computer is just spassing 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 guys (how come there are very few girl hackers?) password, 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 immitate the OS so that no one call tell they're not in the OS. Now when you start you're 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 you program, and then have it print out whatever junk 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 something out before it pretends it finishes, so that it looks like your program does something legit.

Now you have your program running, but it looks like the OS. So the nect 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 until he types it in correctly, 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 you 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 or 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 operator will discover what you 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 is the hardest part to get away with. 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 the log out will look 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 fowarded 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-1", by Thomas J Ryan. P-1 is a heuristic computer program, with a tendency to take over the operating systems (OS) of large computers, especially ones 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 increase 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 First Class subscribers may not like 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 in 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 neard about a book called the "Radio Engineers Handbook", which contains specs on all sorts of electronic stuff. including phone systems. They have info on frequencys, standard impedances, and such. I don't know who publishes it. Also. the IEEE (Institute of Electrical and Electronic Engineers) and the EIA (Electronic Industries Assoc) publish handbooks of electrical standards, which include the same type of stuff. info on normal electronic circiuts 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 that exchange. 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 be able to identify the machine they are using, and you would have a good 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 TWX 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 1KAA1243. How do you convert that number 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 Jester, c/o TAP.

Any of you who have apple micros might be interested in getting the apple-cat modem. It is like a normal modem, 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 recieve touch tone data. This would allow you to use your computer from any phone without a terminal, by simply using touch tones 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 8BBS #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 8BBS #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 BBS it CBBS/NW also up 24 hours, in Portland, OR., at 503-646-5510. These both have phone phreak type of stuff on them. I've seen lists of Sprint codes on 8BBS. Don't put on 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 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 sinoe 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 5 to 50 ms long. If anyone in Orange county can detect these pules, let us know!

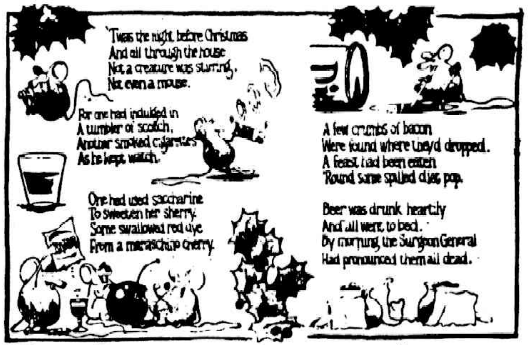
As I'm sure you all know, Bell is slowly but surely going to out of band signalling. This means that I will have to throw away my blue box in a few years, and if I had a black box I'd have to dump that too. In fact the only box that may be of any use will be the red box. Fortunately, Sprint and the other alternate calling networks are filling in gap caused by out of band signalling. There are four alternate calling companies, Southern Pacific Communications (sprint), ITT (citicall), 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. By far Ma Bells lines are much better quality, 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 persons 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. None that I know of go international yet, although Sprint is planning to soon. Sprint goes to the most places in the US, 138 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 them up in its March 1981 issue, available at any library.

Alternate nets can be just as dangerous as a Bell if your 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 MCI, then I have MCI call Sprint in SF. I then go through Sprint and make a local call in SF. This way MCI 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 net, beause 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. MCI is known to do that. You could be busted though, under wire fraud and breaking FCC regulations, both federal crimes. Also in California, there is a law against computer crimes. It is very tough, 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 charge you with. Many other states have computer crime laws too, I'm not sure which ones do. But don't worry, they'll get you on the federal rap anyway. So don't get caught. Ma Bell Security works with the alternate calling companies security divisions, they will trade numbers and info, Bell has even been known to makes busts for Sprint.

One thing you may want to try, it still works in a few places, is calling through on an alternate net, then blue boxing the line going out of the alternate company into Bell. You then get a Bell dial tone on the outgoing line, which you can MF through to. You can go overseas or whatever. There are 2600 Hz notch filters on most alternate calling inputs, but not all.

If you have a micro computer, you can break Sprint (and other) codes very easily. Hook up a modem or even an audio interface to your phone line and program your computer to scan through possible codes, untill 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 Phun Phreaking
Simon Jester


'Twas the night before Christmas
And all through the house
Not a creature was stirring,
Not even a mouse.
For one had indulged in
A tumbler of scotch,
Another smoked cigarettes
As he kept watch.
One had used saccharine
To sweeten her sherry.
Some swallowed red dye
From a maraschino cherry.
A few crumbs of bacon
Were found where they'd dropped.
A feast had been eaten
'Round some spilled diet pop.
Beer was drunk heartily
And all went to bed.
By morning the Surgeon General
Had pronounced them all dead.

Getting wrong numbers

Fallacious mathematical reasoning is one of the most prevalent destructive forces in our society today. It has spread like a cancer through the highest offices in the Reagan Administration. This has not been a major source of concern to Americans, however, because faulty thinking has always been a hallmark of government.

What should be a source of concern to Americans is the spread of fallacious reasoning to a truly important and powerful institution — the Phone Company.

The Phone Company has been playing several commercials recently about the overuse of directory assistance. Perhaps you have heard them. One of the commercials has two people talking, who, for convenience, will be called Lazy and Wrong.

Lazy calls directory assistance to get a number which he could have easily looked up himself. Wrong chastises Lazy, saying that directory assistance is expensive. Lazy says that Wrong is incorrect and that directory assistance is free. Wrong says that directory assistance costs $50 million in Massachusetts alone last year, and that all phone users must share this expense. Not surprisingly, Lazy is so shocked by this figure that he readily agrees to use the phonebook next time and never again to use directory assistance.

So where is the fallacious reasoning, you ask? Suppose that everyone agreed not to use directory assistance. If directory assistance in Massachusetts (population about 5.7 million) costs $50 million a year, then directory assistance in the United States (population about 224 million) probably costs about $2 billion a year — a remarkable one tenth of one percent of our Gross National Product.

With no one using directory assistance, some 150,000 directory assisters would lose their jobs, along with some people who make radio commercials, and the resulting recessionary shock would be devastating to an economy already suffering from oppressively high interest rates.

Furthermore, directory assisters, like the former air traffic controllers, have a skill which is not of much use in other industries. They would have no choice but to go on the Federal dole. Since the Federal dole is being severely cut back, however, many ex-directory assisters might have to go without food (or at least touch-tone service). Riots could ensue.

Admittedly this is a worst-case scenario, but it does highlight the danger of fallacious mathematical reasoning leading to an incorrect economic policy. A policy of using directory assistance as often as possible, on the other hand, would put Americans to work, strengthen the economy, and maybe even bring about lower interest rates. Phonebooks would perhaps become obsolete, conserving a dwindling natural resourse — trees. Clearly the Phone Company's reasoning was completely incorrect. The overuse of directory assistance is not a problem, although underuse may be.

Since MIT is presumably an institution designed to promote correct thinking, we must set an example for the rest of the state and the rest of the country. We must use directory assistance whenever possible.

Remember, all it takes is three little numbers, 411. America can become a great nation again, but only with the *Phone Company's* assistance — and yours.

A scheme you can bank on

Oceanside, Calif. —A lazy robber made some easy money by posting a sign directing bank customers to make their deposits in a bogus deposit box. "We won't know how much was lost until people realize their money wasn't deposited," police spokesman Bill Krungelevich said Friday. Krungelevich said the thief put a note on the outside deposit machine at a First California Bank branch. The note said, "The night deposit is out of order—please leave your deposit in the box." Branch manager Bill Reedy said two women who left their deposit cash in "a shabbily built wooden box" have complained to him.

If you want to cut your phone bills, cut out this chart.

Back Issues are $.75 each. Issue #50 is $1.50.
Subscriptions - 10 issues - US Bulk Rate $7.
US Bulk Envelope Rate $8.
US First Class in plain sealed envelope $10.
Canada & Mexico First Class $10.
Foreign Surface $8. - Foreign Air Mail $12.
IMPORTANT! Please include your mailing label or a Xerox copy whenever you write to TAP about your subscription.
Electronic Courses - $.75 each. A - DC Basics, B - AC Basics, C - Phone Basics, D - Amplifiers.
TAP "Ma Bell" Patch - $1.50.
TAP "10th Anniversary" Pen - $.50.
TAP Cassette Tape - $4. Hear Capt Crunch. Al Bell, Joe Engressia & Bell Security Chief John Doherty.
Send CASH, check, or money order to:

TAP, Room 603, 147 West 42nd Street, New York, N.Y. 10036.

Classified

Up to 20 % MORE M. P. G. 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 S A S E to Box # T.

Continental Spectator

IN OUR 17th SWINGING YEAR

EVERYBODY SWINGS WITH "CONTINENTAL SPECTATOR"

.... 132 full-size pages loaded with personal ads and wild nude photos
.... Nationwide listings - many with addresses & phone numbers
.... Sexy couples, pretty girls, gay & bi males who want to meet YOU
....PLUS swinging articles, stories, readers comments, places to meet swingers and MORE

For a copy of the latest issue mailed 1st class, send $6.00 to: CONTINENTAL SPECTATOR, Room 603, Dept. T, New York, NY 10036.
Please state your age.

PICK LOCKS

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

PICK CONFIGURATIONS PROGRAMMED TO CONFORM TO AN AMAZING 98.6% OF ALL 5 & 6 PIN (STANDARD SPOOL INCLUDED) AND DISC TUMBLER LOCK COMBINATIONS. AVERAGE OPENING TIME 3.30 SECONDS

COMPIX: Set of 12 picks (20 configurations) and 3 tension tools. Top grain leather case and complete instruction manual.

PICK: Type 30 extra hard polished spring steel C48.5 Rockwell tensile. Carbon Range 90/103. Innovative construction permits full clearance thru the most restrictive keyways. Also allows complete freedom to manipulate without disturbing already picked tumblers.

2 Picks (4 configurations) open 83%. Remaining 16 configurations will open diverse L/H combinations.

HANDLE: Cast aluminum base with enameled finish. Comfortable vinyl grip cover.

TENSION TOOL: Three separate designs provide absolute uniform torque for most lock mfrs. - core and tool are made to move as one. Minimum keyway obstruction to pick travel.

PRICE $38.50

COMPIX
1478 California Street
San Francisco, CA 94109

TONTI SYSTEMS

537 Jones Street [illegible]
[illegible]

ELECTRONIC SURVEILLANCE

Preassembled/Project kits complete with all needed component accessories.

Autostarts, VOX, Ultra-sub-mini-transmitters, Linemans Handsets, TPG Systems - MUCH MORE!

Send $1.00(refundable) for the most fascinating catalog of "Confidential Electronic devices" available anywhere.

*Also now stocking a complete line of HPC professional locksmith pick-sets and other trade tools and books. Please indicate if interested.

TONTI SYSTEMS 537 Jones St., #0016
San Francisco CA 94102.

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-M10 (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

YOU CAN

SURVIVE!!

WITH BOOKS FROM TECHNOLOGY GROUP! COVERING URBAN, RURAL & RETREAT SURVIVAL, AND MANY OTHER SUBJECTS AS WELL!! Discounts to 60% on some titles.

DEALERS WANTED !!

List $2 (refundable with order).
TECH-GROUP, Box 3125,
Pasadena, Calif. 91103 USA

Hi there,

I'd love to hear from the women who read this ad. I'm shure some of you read TAP. Please write and tell me about yourself. I'm a 25yr old male radio-tech.

P.O. Box Midnight c/o TAP

ALTERNATE IDENTITIES, NAME CHANGES, WHATEVER. GET LEGAL I.D.S WITH OUR GOODIES. ALSO LAW ENFORCEMENT TYPE I.D. CARDS [23 DIFFERENT KINDS], BADGES & ACCESSORIES. LIST $1.00 (REFUNDABLE WITH PURCHASE). C.W.L. BOX 3230, PASADENA, CA 91103

GUERRILLA WARFARE!

"The Citizen's Guide", New 4th Edition. MORE Color and B&W Illustrations. Re-organized Appendices. 200, 8½X11 inch pages, plus full color cover. $30.00 ea. ABSOLUTELY UNIQUE! Info. & Catalog $1.00 (refundable).

Up-date Kits for older editions available.

TECH-GROUP
Box 3125, Pasadena, CA. 91103

10% OFF TO TAP SUBSCRIBERS!

BEAT THE GAS PUMP

and strike back at BIG OIL! 18 ways of getting fuel FREE or at greatly reduced cost.
23 photos, 6 line drawings.
Big, 8½ x 11 pages.
Written by former Big Oil employee.
$25.00 each

DEALERS WANTED!
List $1.00 (refundable)

TECH-GROUP
Box 3125
Pasadena, CA 91103

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 ad sheet. The cost per ad 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. This extra cost is for the postage to mail you the replies to your ad. 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.**

SOLD FOR EDUCATIONAL PURPOSES ONLY

GAS FO' ALL!!

FED UP WITH THE HIGH COST OF GASOLINE AND DIESEL FUEL?? SICK AND TIRED OF BEING ROBBED AT THE PUMP EVERY TIME YOU FILL UP?? The ultimate energy survival publication is finally here!! We have penetrated the top secret files of the 8 Billion oil companies to pry loose 15 effective simple, quiet and quick methods of ripping-off gasoline and diesel fuel at the pump!! No special skills, strength, aptitudes, luck, intelligence or prior training is required.

GAS FO' ALL!! Completely describes and illustrates (including many photographs) these 15 eye popping methods, applicable to ALL MECHANICAL AND ELECTRONIC GAS AND DIESEL PUMPS AND DISPENSERS. One method stops the registration (but not the fuel flow) simply by placing a strong permanent magnet on the outside of the pump!! Most methods require a few simple hand tools.

GAS FO' ALL!! is ONLY $19. ORDER TODAY! This new, copyrighted publication is so extremely controversial that we cannot guarantee later availabilities at any price. SOLD FOR EDUCATIONAL PURPOSES ONLY. NOTE: We do not sell, trade, lend, lease or give away our mailing lists. Pay $2 extra for insured mail of this and the rest of your order. Free brochure of our dozens of other survival publications sent with order (otherwise $1).

Consumertronics Co.
P.O. Drawer 537, Alamogordo, NM 88310

TAP, Room 603, 147 W. 42 St., NY 10036

"TOO MUCH OF a good thing can be wonderful!"—Mae West

Bulk Rate
U.S. POSTAGE
PAID
Permit No. 3
Keasbey, N. J.