On TAP

by

TOM A. EDISON

On behalf of myself and the TAP staff let me wish all our readers a healthy, happy, and prosperous 1983 NEW YEAR. As has been my policy for the past few years, my initial column is geared primarily for all of our new subscribers, however, all of you long-time subscribers should read it too. The TAP office is being swamped with what I call "error" mail. This mail is wasting the valuable time of the TAP staff. To help ease the situation, let me again state TAP policy. Free subscriptions are available to prisoners ONLY, providing they list a prison address. Free back issues are NOT available to prisoners. The postage is very expensive and most prisons won't deliver them anyway, especially after they've opened them up for inspection and seen the type of information that is in them. Our current number of free prisoner subscribers is large and the cost for this service is being shared by all. If you are unemployed and cannot afford a subscription, send for your issues one at a time. If you cannot afford $.75 a month for an issue, you are in even worse financial shape than you realize!

Payment MUST accompany all orders. PLEASE print or type your name and address. We cannot read your scribbling and chicken scratching which you call handwriting. If we can't read your order, don't complain to us that you didn't receive your order! And please write your name and address on your letter. A number of you lazy bastards are just sending in a check with no other letter of instructions. How the hell are we supposed to know you want? If your check is sent to our bank before we've had a chance to get your name and address off of it, your order is lost! We are receiving a lot of mail with no addresses on it. Again, if you don't list your address, how the hell do we know where to mail your order?

EFFECTIVE JANUARY 1, 1983 TAP subscription rates are $8 for a Bulk Envelope sub and $10 for a First Class sub mailed in a plain white envelope. We have eliminated the old bulk stapled rate. It was too time and energy wasting. Please note that all TAP subscriptions and orders are prorated. If you send in an insufficient amount of payment you will get your order proportional to the amount of your payment.

We are getting stuck with a lot of rubber checks from you cheap bastards! EFFECTIVE IMMEDIATELY: all personal checks MUST clear your bank before we will ship your order. Orders accompanied by certified checks, money orders, and CASH will be shipped immediately. Remember, the 10% discount applies to CASH only. It does NOT apply to checks or money orders made payable to cash. CASH refers to the green currency of U.S. vintage supposidly backed by Big Brother in D.C.

When you RENEW your subscription, please send us one of your mailing labels, preferably the latest one. The code numbers and letter in the upper right corner help us to locate you on our computer list. I have been asked a number of times by readers just what those code numbers and letter stand for. The first number is the first issue number of your subscription. The next number is the first issue you will miss if you do not renew. The letter is your sub type: "B" for bulk; "F" for first class; "E" for export; "C" for Canadian. Some of you have an "E" on your labels. This stood for an experimental sub type : the "Elite" first class sub. This is being phased out and will eventually be replaced by the letter "F".

We mail two issues in each mailing to save on postage. Two issues weigh under one ounce. Issues are published monthly except for the summer months when we take a well deserved vacation. All subscriptions run for ten issues and are mailed around the beginning of January, March, May, September, and November.

Readers are incouraged to send in news clips, items of interest, and written articles for publication. All articles MUST be typed or computer printed using a five (5) inch type column width. Any other format will be rejected. Newspaper and magazine articles and/or clips can be ANY size. We use these as fillers and need various sizes.

I hope this clears up some of the things you new readers wanted to know about TAP. Feel free to write to TAP anytime. TAP is YOUR newsletter!

MA BELL IS A CHEAP MOTHER

TAP

TAP
ROOM 603
147 W. 42 ST.
NEW YORK 10036

JANUARY 1983 No. 81

Security Alert !

by Oz Y. Mandias

Your telephone toll records (the listing of your long distance calls that accompanies your bill each month) provides a handy diary of who you know (& know well), where you are going or have been, etc. These are available without warrant to the pigs and can & are used against you if you're suspected of hanky-panky by the man. They're great for linking you to others in a conspiracy or finding you if you decide to take it on the lam. "Skip tracers" (bill collectors and other free-lance pigs) also find them useful for the same reason. So if you play around or like your privacy, take note & use pay phones (and not always the same one). A word to the wise.

To all dope chemists, or would-be dope chemists, let me reiterate: buying chemicals (especially watched precursors) from an above-ground chemical company IS A BUST sooner or later - and probably sooner, for that matter. The company is usually either a DEA sting operation or cooperating with the narks. A Michigan TAPer who learned the hard way from Merrill Scientific suggests burglarizing either a college chem lab or chem supply house to avoid these pitfalls. A Texas TAPer who says my warning saved his ass, sent in a piece from the Dallas Observer (22 Sept/82) about Georgia Lab Supply (a DEA front out of Decatur, Ga., who fished for suckers by running ads in High Times & Rolling Stone). In the case described, a tracking "beeper" was hidden in a magnetic stirrer to keep track of the conspirators when they picked up the shipment of chems & equipment. Universal Solvents out of Chicago is another sting operation to be wary of.

Remember, to get chemicals: 1) steal them, 2) have an inside contact at a chem company get them, 3) have an inside contact at a company that legitimately buys the chemicals you desire, 4) use several separate "mules" & pass the chemicals between people & locations over a period of at least 6 months, 5) synthesize your precursors from simpler unwatched chemicals, or 6) synthesize a legal analogue.

The drug outlaw should also be aware that the recent merger of the FBI & the DEA probably spells trouble with the use of the FBI's more sophisticated investigative methods, such as wiretaps & use of financial records, which the DEA often ignored or botched.
The R.I.C.O. & Continuing Criminal Enterprise (21 USC848) statutes are also coming into vogue against dope criminals. They require precious little proof & carry time measured in the decades.

A new bug used by law enforcement types is designed to thwart de-bugging sweeps with RF detectors. This device utilizes a spike microphone (a contact or remote mic may also be used) to pick up conversation from the targeted room externally, through the wall. The mic input is now used to modulate an infra-red beam which is aimed at a line-of-sight IR receiver 50-75 yards away (on the top of a telephone pole is favoured), which picks up the beam with a IR photocell, recovers the audio-freq. signal, and then retransmits it on a standard RF transmitter.
The purpose of this round-about way of eavesdropping is to avoid having a source of RF energy in the room or in the immediate vicinity that may be picked up in a sweep with a field-strength meter. Only a good (inside and outside) physical search of the premises will uncover this type of bug.

And speaking of invasions of privacy, an article in Science (3 Sept/82) details the methodology of wiretapping by intercepting the signals of microwave relay towers. The specifics of this are detailed in advanced terms in the NTIS publications I mentioned in an article some time ago.

This has been Oz Y. Mandias, reminding you to live fast, die young & leave a good looking corpse.

BUYING CHEMICALS by Dr. Atomic

As you may know, buying chemicals and reagents is not as easy as walking into Radio Shack and buying a bagful of resistors and diodes. For one thing, Radio Shack won't call the DEA on you.

The technologist who seeks chemicals for his hobbies, whatever they may be, if he does not follow established buying procedure, is automatically assumed to be an illegal drug manufacturer, and the Chemical Supply House (CSH) sales agents will call in the DEA to investigate.

To avoid repeating others' mistakes, it is helpful to know what doesn't work. The most common method of purchasing chemicals that does not work is a method I call the "Get The Chemicals And Try To Shake Them" method. In this method the Technologist goes into the CSH "cold" to make a purchase. He suspects that they will call the authorities on him, but he thinks that he can shake the surveillance. Although it can be done with some James Bond style tactics, the failure rate is high, perhaps as high as 75%. Dr. Atomic does not recommend this method.

Sneaking by the CSH sales people is difficult. To give you an idea of what you are up against, here are a few things that they watch out for: new accounts; cash purchases; out of town customers; individual (not corporate) purchases; all orders for drug precursors; customer pick ups; hippy appearance; and lack of expertise in using the nomenclature of chemistry.

The second most common method of obtaining chemicals that does not work, in many cases, is buying on the Black Market. The reason why the Black Market is no good, in general, is because the DEA is out there selling precursors (or fronting them), hoping to lure in some unwary technologist. Beware of sting operations, many of which are run through classified ads. Although you may know the guy you are getting the chemicals from, if the DEA is involved anywhere along the supply route, you'll probably pick-up a conspiracy charge (thought-crime), which carries a penalty of 5-15 years. This is no game.

Now that we know what doesn't work, here's the method that has a better probability of success. I call it the "Inside Job". It's simple: get a job at a place that has the chemicals and help yourself. CSH's, manufacturing industry, and labs are good choices.

If you aren't able to do the Inside Job yourself, check your list of friends to see if you have someone who can get the chems from where he works. If you don't have such a friend already, perhaps you can arrange to have a friend infiltrate some business with the chems. The rule is that you have to keep control of your line of supply and not have any police or informers in it.

The inside job has many possibilities. For example, one could start his own company and run "the siphon". The manufacture of perfumes, essential oils, and insectisides are business that use a wide range of chemicals. To be successful with this approach, one has to actually carry on a legal buisness. It's a lot of work, but you secure a long-term, relatively safe source of supply.

I have stated this before and will repeat it here again because it is important: ALL CHEMICALS ARE WATCHED CHEMICALS. Some are hotter than others, of course. But all of the immediate drug precursors such as phenylacetic acid, benzyl chloride, and methylamine will almost always set off an alert. If you are ordering precursors to your business, you must be able to justify their use in your manufacturing or sales process.

The days of just walking in and buying chemicals fast and easy are over. There are no fast ways, for all practical purposes, to safely buy chemicals other than by having a friend "inside". The grim reality that we must face is that the practice of chemistry is in effect being prohibited to individuals.

It is said that freedom of the press belongs to he who owns the press: likewise, freedom of the practice of chemistry belongs to he who controls his source of supply -- or owns it.

ATM TECHNOLOGY by Jolly Roger

Many banks and S&L's are now issuing debit cards as well as credit cards. These debit cards allow withdrawals from one's account either over the counter or from Automatic Teller Machines (ATM's).

The Personal Account Number (PAN) is embossed on the card, while the Personal Identification Number (PIN) is encoded on the magnetic stripe glued onto the back of the card. Since the PIN number is supposedly known only to the holder, if the card is lost or stolen it still cannot be used.

Usually the holder of the card inserts it into the ATM, punches in his PIN number (sometimes the PAN number as well), and the machine scans the card and relays the information to a computer via telephone lines. If everything checks out the money is issued.

Daily limits vary and can be as low as $100 a day or vary with the size of the account. ATM's are truly the wave of near term banking future, and tens of thousands of them are being installed all over the world each year due to their success and popularity.

There are generally five ways a machine is protected: 1) primarily by the secret, encoded PIN number; 2) limits of daily withdrawals; 3) automatic card confiscation by the machine under certain circumstances; 4) photos taken of the user by the machine; and 5) silent alarms.

It is interesting that stories appear where a machine "goes crazy" and coughs up lots of money to someone that turns it back into the bank, but the stories of fraud are not printed in the media or even shared between banks usually.

The machines can be defeated thru several strategies such as stealing the card from the cardholder and decoding the PIN, having a debit account and denying your withdrawals by having someone else use your card, employees within the bank stealing lists of PAN/PIN numbers and making up bogus cards complete with mag-strip, putting false fronts on the machines to collect cards and money from legitimate users, tapping the phone lines with a tape recorder and replaying it the next day, tapping the phone lines and deciphering the code and feeding in your own information, working in the bank and programming the computer to think your account has more money in it than it really does, or for the real wizard to figure out an electronic device that would tap in the phone lines and order the machine to simply empty itself. There are other methods only limited by the imagination.

About the most practical and productive way is simply to photograph users of ATM's with a telephoto lens and portable video tape movie camera, replaying your movie at your leisure and copying down all the PIN and PAN numbers. Then, one can take plain blank plastic cards and use an encoder machine to put the information magnetically on tape and glue it to the cards. The tape has the PAN number, PIN number, and lastly a "check digit" derived from the foregoing two numbers.

Any good book on computer technology for credit cards will explain how to figure check digits. Get your own debit card from the bank and decode it to make sure you are using the same formula for the check digit.

You can decode mag-strips by using a "reader" connected to a "writer" available at electronics outlets, or by placing chromium dioxide tape over the mag-strip and heating it with a 300 degree iron to transfer the information, or by using a magnetic developer to produce a hard copy of the encrypted data.

Reading the right books will answer any questions you have about encoding, decoding, encryption, check digits, or whatever. Encoding machines are available from companies that sell "Credit Card Equipment & Supplies" in your Yellow Pages.

For the less imaginative a LAW rocket will probably loosen up the money cartridge from a suburban ATM very nicely.

The ARPANET
(Part III: General Netnotes)

by Fred Steinbeck

This is my last column in the ARPANET series of articles, although there may be occasional updates in the future. This column will try to cover miscellaneous information that didn't fit anywhere else, and things like that...

SRI's Services

The Network Information Center (NIC) at SRI can be very helpful in nethacking. The last column mentioned the NIC computer (host 0/73), and talked about using that for getting information on the ARPANET.

However, SRI has other functions. First off, they publish two excellent books. The first, the 1,020 page **ARPANET Resource Handbook** (NIC document number 47500), tells all about each computer connected to the ARPANET. This book also lists the network liaisons (people who are the resident gurus at various places connected to the net) and how to get in touch with them.

Another book is the 560 page **ARPANET Directory** (NIC document number 49000). This book lists all the legitimate (and sometimes illegitimate) users of the ARPANET. This is the book that I use the most, as it is more current than the **Resource Handbook** (March '82 as compared to February '80 for the Handbook). The Directory also lists the physical locations of TIP's and TAC's, and many other useful things.

These documents can be ordered (free, no less) from the NIC at SRI International. They prefer ARPANET mail, so if you have access to the net for mailing, send a message to NIC@SRI-NIC. If you must, phone (415) 859-3695, or Telex 334463. If you do any of these things, be prepared to look official...

Oh, yeah: ask to be put in the ARPANET directory. They used to have an (intelligent) policy of limiting the people in the directory to authorized users, but then they started allowing anyone to be put in it. Mail to NIC@SRI-NIC and include your name, physical mail address, network mail address, and your phone number.

Good Computers

There are a number of good computers for nethackers. The first, and the most famous, is the Artificial Intelligence lab computer at MIT (MIT-AI). This is host address 2/6. There is a program there which you will want to run, called ACOUNT. This allows you to get a guest account on the system. Unfortunately, at the time of this writing, the MIT-AI system was scheduled to be taken off of the net and replaced with MIT-OZ, which has better account security.

If you do manage to get on the system, there is an INFO program which will teach you many things about the ARPANET, and while it is obnoxious to use, it's very educational.

Another good one is the Stanford University Artificial Intelligence Lab computer (SU-AI or SAIL). This is host 0/11. SAIL has an extensive help library (just type "help") and you can learn a great amount here, too. Also, one of the help commands ("help help" gets a list of topics) produces a huge list of various computers connected to various networks (including some phone numbers).

Government Computers

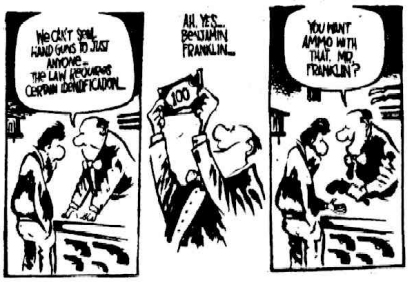
For those of you who are into breaking government computers, you may want to try some of these systems:

Coins-Gateway, host 1/57. This computer allows access to the Community Online Intelligence System (COINS), which is a subnet of the ARPANET. COINS itself allows access to a restricted subnet of the COINS net.

Tycho, host 0/57. The Tycho computer is run by the National Security Agency. I have no idea what it does, as the only information I have on it is a 6 line description which tells nothing about it.

PENT-UNIX, host 3/26. This computer is used for "text processing and administrative support" (yah, I bet...) by the Air Force Data Services Center, The Pentagon. I have heard that this system was penetrated by a phreak and nothing interesting was found, but he could have missed something.

These are only some of the governmental computers connected to the net. I wouldn't be surprised if there are more systems on the net than they say there are... So go wild, people! Find those systems and report 'em to TAP



More UNIX Wizardry

by Fred Steinbeck

Okay, as promised in issue number 79, here is another interesting thing which can be done to what just may be the world's least secure operating system: UNIX. Actually, I suppose the honor of "least secure OS" has to go to the ITS operating system, developed by MIT, but who cares?

Anonymous Messages

Ever wanted to leave a message advertising TAP on your UNIX system, but didn't want your name associated with it? Well, here's how to do it and remain safe from the "authorities".

On UNIX, to put a bulletin in on the system bulletin board, you give the command "Mail msgs". Well, as it turns out, there is no mail account called "msgs". But if we check the file /usr/bin/aliases, we find a list of mail aliases. That is, this file contains all the aliases which cause mail to be delivered to somebody else instead of who it was mailed to.

It so happens that there is an alias for "msgs", and it translates to the program "/usr/bin/msgs -s" which is the program to post messages on the bulletin board. The "-s" tells it to post the messages, not to read old ones.

Anyway, first create a file which looks exactly like one generated by the Mail program. That is, one which has a "From: blah", a "To: blah" and a "Subject: blah" field in it - look at any letter you've received and copy that pattern. Anyway, change the "From:" header to a suitable, non-existant name like "phreak", the "To:" field to read "msgs", the subject to whatever you want, and then save the file (which we will call "file", for sake of argument).

Then give the command:

```
cat file | /usr/bin/msgs -s
```

which will put the message on the bulletin board. This proved handy when I broke into a U.S. Geological survey computer and put up some TAP ads. Didn't surprise me much that the next day the passwords for all accounts were changed...

CREDIT CARDS

by Simon Jester

You have probably heard that Bell is going to eliminate third party billing soon. Very soon. As early as January 1983 in some places. They claim that there is too much phraud. So they are only going to allow collect and credit card calls from pay phones. That was the good news. Here's the bad news. Bell is changing the way credit card codes will be made up. Reliable sources tell me that the new CC's will still contain your area code and number, but the RAO code and check digit will be replaced by a three digit code. **The object, of course, is to keep us from making up cards.**

Some sources say the new codes will be random, and cannot be determined simply from knowing the phone number, while other people tell me that the new codes will be created from the number, like a very complicated version of the present check digit system. Bell would prefer totally random codes, because they would be almost impossible to break. But it would require an operator to verify every card every time a CC call is made. This would require a very large computer system. It is not beyond Bell's capacity, but it would certainly be very expensive. If the code is created from the phone number, it would be possible for each operator (or a small micro) to check each code without a large central computer. A much cheaper alternative, but not as secure, as we would eventually figure out the formula used to make up codes. I tend to think they will opt for the completely random codes, but it is hard to tell, and the upcoming split into 22 seperate companies makes it very hard to predict what will happen. If anyone of you faithful TAP readers learns anything about the new CC system, please write it up and send it in.

You may have seen those blue payphones Bell is installing that don't take money, but only allow you take make collect or CC calls. Many of them will allow you to make a CC call without ever talking to an operator. (Some regular payphones work this way too now) You just dial 0+area code+number, and a recorded voice comes on and tells you to punch in your CC number or 0 for a human operator. You usually get 2 chances to get the code right. This is a quick and easy way to test CC codes and see if they are still good. I have also heard that when the new CC system is put into effect, you will be able to go up to the blue payphones, and put in a special code instead of the regular 2 digit code on certain cards, and you will get special abilities. I have no idea what these abilities are or how this works, but it is designed for internal Bell use only.

Until the new CC code system is put into effect, here's a hint on getting good cards. Bell is trying to get everyone to use their "calling cards" (their name for Bell credit cards), so the cards are free and using them is cheaper than most other operator assisted calls. But often the operator not only checks to see if the check code is good, but to see if the card really exists. This means it is useful to have a real credit card code available when neccesary. So have Bell make up a real code for you, like this: look up some number in the phone book, call up the appropriate billing office, and request a CC for that number. Be sure you know the name, address, and phone number you are supposedly calling from. The card itself is free, so it won't show up on the guys bill. When the card shows up in his mail, he may ask Bell what it is, and they'll tell him, but they will probably suggest he keep it in case he ever wants to use it. You, of course, have made up his complete CC code (including RAO code and check digit) and can now use a real genuine Bell credit card. When he gets his bill with all your calls on it, he will complain to Bell who will take the charges off and absorb the cost of your phone calls. The card ought to be good for a few months before it is turned off. Remember to only call people who have short memories of who called them, or call payphones. This system ought to keep you all in CC codes until the new CC system is put into effect. If you don't know how to make up a CC code for a phone number using the RAO code and check digit, write to Tom for a copy of "TAP fact sheet #1: Credit card calling hints", 50¢ a copy. See Tap #72 for the 1982 check digits.

Technology Illustrated-
What that was about, anyway.

by Cheshire Catalyst

A few months ago, I was contacted by an editor of Technology Illustrated magazine in Boston. They had heard of us through a freelance journalist in Boston, and wanted to do a feature story on the "Technological Underground", and we were the closest manifestation of this that they could find. After all, the "Computer Criminals" that get away with all manner of evil deeds can't be found, and wouldn't want to be written up in any case.

TAP's philosophy in such instances is to provide information to anyone who requests it. TAP is, after all, the keeper of The Forbbiden Knowledge, or at least the knowledge that Bell, and other utilities and corporations and governments don't want you to know. We normally try to keep a low profile so that Bell and the others won't think us a target worth bothering about, and so we generally try to have the word of our existance travel only by word of mouth. The only times we've gone out seeking publicity was for the Phone Phreak Conferences we've occassionly held over the years. Then, we needed to get the word out so that money we sunk into the conferences out of our own pockets would at least come back, and we'd break even.

In cases where Gentle Persons of the Press have written in seeking us, I've sent out our little press release ("For Release On Request") to the people requesting the info. Some have stopped down for a beer with us, and have even gotten something into print. Others just had a beer. While we've been written up in The Washington Post, Infoworld, The Silicon Gulch Gazzette, and even Business Communications Review (which refered to me as "one of the counrty's best known Phone Phreaks." Thanks for the compliment Jerry) as well as other publications, we've never gotten the response from any of them as we've gotten from the article in the October issue of Technology Illustrated.

Reaction was immediate in some circles. I lost my job with the "Large Manhattan Firm" that I used to work for, and Technology Illustrated lost the Bell System as advertisers. As a result, I am available for consulting on how easy it would be to enter remote computer systems, and Tech Illustrated would like to get advertising from any other telephone common carrier. If your company doesn't like Bell, suggest to your advertising department that Tech Ill might be a good place to drop an ad or two.

Alot of people have written to ask how the photographs were done. The lead photo of me in front of a New York City pay phone was taken on 43rd St between 5th Ave and Avenue of the Americas (6th Ave to us New Yorkers). I had a rectagular mirror hot-glued onto a pair of sunglasses, and I was reflecting the evening sun back into the camera lens. The shot of The Gang was taken in front of the Greenwich Village restaurant where we gather on Friday's after work. If you plan to be in New York on a Friday, write and ask where to show up. The photographer set up his camera on a tripod, set a high F-stop, set a multi-second exposure, and as he snapped the shutter, we all shook our heads. For those of you unfamiliar with New York, the silouette shot of me was taken against the background of a moving subway train. I was (I have to admit) rather embarrassed by the shot of my room, but once the photographer saw it, he said he had to shoot it. He said it captured "The essence of the Information Maniac."

If you missed the article, I still have a few copies left, and will be happy to autograph one for you. Send $2.00 (for the magazine) and $1.50 (for postage) to Cheshire Catalyst, at the maildrop address.

Birthday bandit

TOYOHASHI, Japan — A schoolboy celebrated his 16th birthday yesterday by using a toy rifle to hold up a bank and flee with $24,000.

Police said the youth, who ran away from home on July 1, was captured by bank employes after a chase.

Pot won't get you in Dutch here

Enschede, the Netherlands —A youth center began selling government-tested marijuana yesterday in an attempt to keep users from moving on to harder drugs.

After two years of debate, this city near the West German border gave the Kokerjuffer Youth Center permission to sell products made from hashish, a concentrated form of marijuana.

A 1976 law gave local authorities the power to tolerate small sales of the drug and also decriminalized possesssion of small amounts, Dutch Justice Ministry officials said.

The authorized dealer here, who said his wares must be tested for quality and purity in an official laboratory, gave his name as Clemens Pot