-==-

THE HIGH TECH HOOD SQUAD PRESENTS...........

```
             AAAAAAA      TTTTTTTTT     MMM        MMM   '''
            A      A         TT         MMMM      MMMM   '''
            A      A         TT         M   M    M   M     '    SSSS
            AAAAAAAAA        TT         MM   M  M   MM         S
           A         A       TT         MM    MM    MM          SSSS
           A         A       TT         MM          MM              S
           A         A       TT         MM          MM         SSSSS
```

THE REAL FILE FOR ATM THIEFT IN 1992!!

WRITTEN BY: THE RAVEN

=-=

NOTE: There has been a few files written about how to 'RIP OFF' ATM's of some sort but this file will not contain technical shit on the card tracks or a xxxyyyooo17ss type of format. This text will tell you how to rip off ATM's with out all of that technical stuff that you can't really use because most of the stuff are too hard. So I give you methods on how you can defeat ATM's with things you may or may not need to pay a-lot for! This file is real unlike a file I came accross that a user uploaded on Blitzkreig called KRAD#1 which I feel was written by 10year olds. That file is totally SHIT! Now there was a-lot of Valid writers on the subject of ATM's but I feel they were on the subject of PINs & PANs which is very hard to do right.

NOTE II: ATM theift is a Federal Crime and the Government doesn't like there funds fucked with. The author does not, DOES NOT bare responsiblity for the misuse of the information, if you are able to commit any of the crimes listed then your able to be responsible for your own damn actions! Dont tell'em I made you do it!

THE RAVEN
+=======+

INDEX

I. Con Jobs
II. Physical Methods
III. Electronic & Computer Scams
IV. Bogus Cards, Getting PINs
V. Authors Note

I. CON JOBS

New York City (My Home!) is the leader in ATM con jobs. Altogether, about 2,000 Citibank users were victimized by ATm con artist in one years time for a tune of $495,000!!So I'm going to spread some light on what and how these cons are pulled off.

Method 1: THE "DEFECTIVE ATM" CON

A con method popular with Citibank ATMs netted one con artist $92,000- with the unwitting assitance of his 374 victims. The scheme works in lobbies with more than one ATM, and a service phone. The well dressed and articulate con man poses as a legit user and stands between two ATMs, pretending to be talking to the bank service personnel over the service phone. After a user inserts his card into the ATMs card reader slot he tells his that the machine is not working. The user withdraws his card leaving the ATM activated. THe con man then observes theuser enterring his PIN into the adjecent ATM. Then, still holding the phone, the con man enters the users PIN into the first ATM. In make-believe conversation with the bank, the con man acts like he is receiving instructions from the bank. To complete the theft he talks the user (major social engineering!) into entering his card into the first ATM again to "test" or "clear" the ATM. He claims that bank personnel think that the user's card "locked up" or "jammed" the ATM and or that ATM may have made the users card defective, and the insertion of it is required to "unlock" or "unjam" the ATM and/or to verify that the user's card is still vaild. After the users leaves, the con manenters into the keypad and withdraws the maximum daily amount from the users account.

This only works on Citibank ATMs cause they don't take the users card, but once the card is slipped in the ATM is activated.

Method 2. PHONE PIN-EXTRACTION SCAMS

Another popular con is for the con man to call up an ATM user whose card he's found or stolen. He identifies himself as a police officer, and obtains the PIN from the user by stating that it is required by law to verify the card owner. This works really well if you can bullshit them good like act like you have to do something and tell them to call you right back (on a loop!) and have a friend answer as the police station!

Method 3. THE BANK DICK CON

A subject was recently was recently convicted in N.Y. and Boston of defrauding ATM accounts of $150,000. He dubed over 300 ATM users into believing he was a bank security officer who needed assistance in the apprehending of a dishonest bank employee. The users were convinced to leave their bank cards under the locked door of the bank. The con man would then "fish" the cards out. The next morning the con man would have someone make a phone call to the card holder saying that they have

caught the employee and dective "hacker" would like to thank you to. But since the employee did come is contact with there card the bank is going to give them a new PIN # after the get the old one! Then the con man's helper would say come pick up your new card and we will tell you your new PIN #.

II. Physical Methods

Some folks just dont like to outsmart a system or person. They prefer the more physical approach by either breaking or removing the ATM. The hazards are obvious-several built-in silent alarms,heavy stainless steel safe like construction, the amount of commotion and noise that results from their efforts, hard to dispose of evidence, etc. Those who have the most success with physical methods, plan and execute their operation as if it were commando mission.

The methods described below can also be used on night depositories, payphones, dollar changers, candy machines, parking meters,etc. Physical attacks must be completed within 10 minutes as ATMs abound with vibration, heat and proximity detectors, and most are silent.

To defeat any internal alarm mechanism,refer to the phone tapping approach (described in detail later) that hooks-up both the ATM and main computer to a programmed micro. So while Hood one is ripping-off or -up the ATM, the micro is whispering sweet nothings to the main computer. NOTE that not all ATM alarms transmit thru the ATM como lines, particulary with thru-the-wall ATMs. To minimize the noise and commotion, heavy blankets(used by movers) can be drapped over the ATM.

Method 1. SUPER COLD GASES

Liquid nitrogen can be used. It is simply poured onto or into the offending part of the ATM and when it hits 100 degrees or so, a sledge or a ballpeen hammer is smartyl slammedin to. THe metal SHOULD shatter like glass. Then one just simply reaches in and examines the untold riches stored inside. Super-cooled gases can also wreck havoc on electronics, cameras and films, and bullet-proof glass, and can be purchased from suppliers of medical and chemical supplies.

Method 2. WATER & ICE

We have also herd that pouring warm water into an isolated ATM on a very cold night is effective. When water freezes, it expands with a terrific force, and will shatter or tear apart anything made by man. The water is poured or pumped in thru the card slot or cash dispenser. It is heavily mixed with wood shavings or fiberglass to stop-up any drainage hole in the ATM. Leaks can also be plugged up with window putty or bubble gum.

Method 3. MORE FREEZE METHODS

ATMs use ACE locks (the ones found on most vending machines, the circle type lock) Freon works on these locks. Somw outlaws empty a can of freon into an ATM lock, pound a screwdriver into the key way, and wrench the lock

out. And motor-driven ACE lock pick will vibrate pins into the right positions withine a few minutes. The ACE lock picks can be aquired from STEVE ARNOLDS GUN ROOM call (503)726-6360 for a free catalog they have a-lot of cool stuff!

Method 4. ACETYLENE & DRILLS

ATMs are notorisly vulnerable to attacks using acetylene torches. With most ATMs no more than 5 minutes are required for the entire job! And most ATMs can be drilled out in under 15 minutes, using carbide bits and high rpm drills (check on my SAFECRACKING text to see more about drilling.).

Method 4. SHAPED CHARGES

Placing shaped charges on each support and detonating them all at the same time liberates the ATM. You can firgue this out by yourself.You can also check most BBS's to find out how to make explosives but I wouldn't recommed it, since most of the expolsive files I've seen are inaccurate and leaves out MAJOR measurements and cautions! Your best best is to use black powder that you can get form almost all gun stores.

Method 5. BLOCKING THE DISPENSER

Some ATMs use money drawers. The ATM outlaw screws or epoxies the drawer solidly shut, at the onset of a busy three-day holiday. At the end of each night he returns and he removes the money by unscrewing or with a hammer & chisel, shatter the epoxy bond.

III. ELECTRONIC & COMPUTER SCAMS

Scarcely a week goes by that I don't hear about one scheme or another successfully used by phreaks & hackers to penetrate large systems to access data banks and to perform various manipulations.

Although we have only been able to verify one or two of the methods that we will discribe, numerous cases have arisen in recent years in which an ATM was defrauded with no evidence of a hardware or software bug to account for the robbery.

The outlaw can use several approaches. One is to use wiretapping. Another is to obtain the secrets of the cipher, or hardware or software defeats to the system and proceed accordingly. Another one that works with banks is to set up phony debit accounts and program the computer to beleive that the debit accounts are full of money. Then when a three day weekend comes around proceed with friend to deplete all of these debit accounts by making various rounds to ATMs.

Electronic frauds of ATMs require an excellent technical understanding of phone and-or computers all of which you can obtain from worthy underground news letters such as TAP, and 2600, etc. OR from a H/P BBS.

"Tapping" or "wiretapping" consists of the unauthorized electronic monitering of a signal (voice or digital) transmitted over a phone or computer (commo) circuit. A "tap" is the monitoring device that does this. Athough a tap is usually placed somewhere on a phoneline or junction box, it may be placed inside of a phone, modem or computer.

With the advent of isolated stand-alone ATMs (with vulnerable phone lines, including POS terminals) and computer technology. The phone circuits that connect ATMs to their host computer (located in the banks data processing center) can be tapped anywhere between the two.

An "invasive tap" is one in which a hard electronic connection is made between the tap and the commo circuit. A "non-invasive" tap is one in which an induction loop or antenna is used to pick up the EMI generated by the signal, and there is no physical connection between the commo circuit and the line.

A "passive tap" is one in which the tap simply tramits to a recorder or directly records the tapped signal and in no way interfers with it. An "active tap" is one in which the tap ALSO interferes (changes,adds to or deletes) the tapped signal in some way. Active taps are more sophisted. A typical ATM active tap is one that records a signal, the later plays it back over the line.

Be sure to look for my text "HIGH TECH TOYS" it lists were to get things that are VERY hard to get or things that you may need a license to obtain without those hassles all you need will be money!

Method 1. PASSIVE TAPS

All tapped ATM transactions are recorded over a period of time (but not interfered with). Once the serial protocal and MA codes are understood, the transmitted data is decrypted (if encrypted) using known entry data to the ATM. Note that some systems use a MA code that is complex and very difficult to crack.

Messages to and from the ATMs host computers are composed of various fields. One field identifies the transaction type, one the PIN, one the PAN, one the amount, one the approval code, one the transaction number and perhaps other fields. In most systems, either nothing is encrypted or only the PIN field. In others, the entire message is encrypted.

The ATM/host circuit is monitored over a period of time to deterive PINs,PANs and other entry data of other ATM users based upon (decrypted) transmitted data. Phony debit cards are then made to defraud ATM accounts with known PINs and PANs.

Method 2. ACTIVE TAPS

Active tapping is one method of spoofing. The c4ritical part of the host computer's message are the approval and amounts fields. The critical parts of the ATMs transmission are the continuous transmission it makes to the host computer when NO one is using it to indicate that it is OK, and the PIN and amount fields. Booth good and bad cards and good and bad PINs are entered at various times and days to differentiate between the various massage components. Various quiescent periods is also recorded.

Once the message structures are understood, a computer is then substituted to act as both the host computer and the ATM. That is, a computer is then connected between the ATM and the host computer. This computer acts like the host computer to the ATM, and like the ATM to the host computer.

An accomplice uses the ATM to go thru the motions of making legitimate

transactions. If his procedures are correct, the ATM communicates, with the host computer for permission to discharge the money. Several methods:

(A) The phreaker changes the approval field in the hosts message to OK the transaction regardless of its real decision. The phreaker may interdict the message regardless of iits real decision. The phreaker may interdict the message from the ATM to tell the host that the ATM is inactive while it interdicts the host message to tell the ATM to disburse the cash. Since the ATM is no longer connected to the host computer, and the host computer believes that it is talking to an unused ATM (or one engaged in balance inquiry transaction), no monies will be deducted from any debit account, no denials will be made based upon daily maximum limits, and no alarm will be sounded due to suspicious behavior. Even if the ATM sounds an alarm, the host computer wont hear it as long as the phreaker is whispering sweet nothings into its ear. Also by using this method, as long as the PIN & PAN check digits are legitimate ones based upon the ATMs preliminary and cursory checks, the PINs and PANs themselves can be phony because the host won't be there to verify legitimacies! That is no legal PINs and PANs need be known nor the algorithm for encrypting PINs.

(B) The ATMs message is replaced by a previously recorded legitimate transaction message played back by the phreaker. The cash is despense as before. The play back method won't work if the encryption or MA process embed a transaction, clock or random code into the message, making all messages unique.

(C) The phreaker/hacker changes the PIN field in the ATMs message to a legitimate PIN of a fat-cat like DONALD TRUMPs account. The phreaker/hacker then withdraws someone else's money.

(D) The phreaker/hacker changes the amount field in the ATMs message to a much lower one, and then changes the amount field in the host's message back to the higher amount (debit transactions- the opposite changes are made for credit transactions). Sooo the phreaker can withdraw $200 from his account with only $10 actually debited from it by the host. He can then make many withdrawals before the host cuts him off for exceeding the daily max.

Method 3. TEMPEST IV

A thin induction pick-up coil, consisting of many turns of one thickness of #28 or thinner enamel wire sandwiched between two self-adhesive labels, no larger than a debit card, can be inserted at least part way inside the card slot of most ATMs. This coil is then used to "listen in" on the electrical activity inside of the ATM to try to determine which signals control the release of money. Using this same coil as a transmitter anteenna, these signals are then transmitted ti the realse logic to activate it.

It is believed that a thin coil about the size of a dime can be maneuvered quite a ways inside most ATMs for sensing purpose, and that small metal

hooks have also been fed into ATMs to obtain direct hookups to logic and power circuits.

It is believe that some outlaws have obtained ATM cards. They then machined out the inside of the cards, except the magnetic strip. They then place flat coils inside the machined out area. They then monitor the coils during legitimate transactions. They can also use the coils to transmit desired signals. This is kind of the method used in TERMINATOR 2.

IV. BOGUS CARD, GETTING PINs

Almost all credit cards now come with either a hologram or an embedded chip ("Smart Card"), and are thus nearly impossible to counterfeit to date. However, since most debit cards are not optically read by ATMs, they are much easier to counterfeit. To counterfeit a card the following is needed:

(1) A card embosser, which can be readily obtained from commercial sources (see "Embossing Equipment and Supplies" or similar in the Yellow Pages) without question asked. A used, serviceable embosser ran use $210 + shipping & handling. (2) A magnetic stripe decoder/encoder (skimmer), which can be purchased from the same company as the embossing equipment or just look in the back of Computer Magazines. (3) PIN checkers are not known to be available to the general public. However, if one were stolen, the user could guess at card PINs by trial-and-error effort based upon the knowledge of how PINs are derived. (4) PANs,PINs and ciphers, which can be obtained from a number of ways usually involving theft. About 50% of ATM users write their PINs either on their debit card or somewhere in there wallet or purse. And most user-chosen PINs are easily guessed. The encrypted PINs can be directly lifted or read from the magnetic stripe, and the encryption scheme determined by comparing the encryption with the known PIN # of a dozen or so cards.

V. NOTE

NOw this text covers the file that I have put together on ATMs but I know that there is more on the subject that I have left out either because I dont want to put it or because my staff: The High-Tech Hoods did get or know the info. now I am open to suggestions for ATM 2 but I dont want any ideas I want proof. !! Then I'll publish it and give credit where credit is due. I can be reached on the following bbs's:

Blitzkreig (502) 499-8933

RIPCO (312) 528-5020

Those bbs's get my files first run!!! C Ya and remember dont get caught!!

Look for my other files:
- Burglar Alarm Bypass prts. 1,2 & 3
- SafeCracking
- Van Eck Phreaking (will appear in TAP)
- Counterfeiting prt 1. & prt 2
- High-Tech Toys Sources List

Comming Soon: Stopping Power Meters
KW-HR METERS ^
Liberate Gas & Water Meters
Cons & Scams
Shoplifting
and what ever you want info on!

THE RAVEN
+=======+