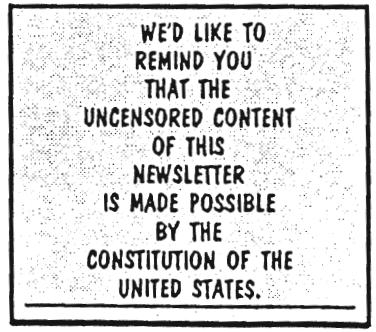
Tap Magazine Issue #104 March 1991

Published since 1971.



$2.00

TAP Magazine
Post Office Box 20264
Louisville, Kentucky
40250-0264 USA

TAP Magazine
Post Office Box 20264
Louisville, Kentucky
40250-0264 USA

Contents

TAP Magazine
Post Office Box 20264
Louisville, Kentucky
40250-0264
U.S.A.

TAP Magazine is published once a month. Subscription rates are as follows. USA is $10.00 for 10 Issues. Canada is $15.00 for 10 Issues, and $20.00 for 10 Issues to any overseas address.

PredatOr: Editor and Publisher

==========

TAP RAP 104 by PredatOr

Since the cost of postage has gone up i decided to save a few bucks and mail issues 103 and 104 together to subscribers who are current. Those who expire at 103 will not get 104 and those sending in at later times will get the issue they request. I was going to start sending out TAP with a hard cover like issue 103 but it is faster and cheaper to use envelopes. I might experiment around some with the next few issues to see which is better but i think i will stay with the brown envelopes.

The small article in issue 103 about Aristotle and TAP needs some explaining. First the reason he put out TAP for free is because he used my copy machine. It sure didn't cost him a penny to print, but it cost me. Aristotle also did not keep very good mailing list records. Some of the people who subscribed when he was the editor have never received an issue. I now am faced with angry letters of "where's my issues?".
I will also explain the reason he dropped out. We both were busted for something unrelated to computers. He thought if he got busted again for TAP he would goto jail. So he turned it over to me. After i became editor he still had the post office box in his name. He would go everyday and get the mail before me and read it, file it away, or who knows what the hell else? Then he says he doesn't want the box in his name, so we get it changed to mine. He keeps getting the mail everyday, yet he claims he is OUT and has nothing to do with TAP. I then had the post office change the lock so only i could get the mail. Aristotle asks me for a key and i told him no. He got mad and has not talked to me since early December 1990. So when you hear his stories about being scared of raids and things like that you now know the real reason behind all this mess. And speaking of messes he will be pissed after he reads this and more then likely more rumors and stories will circulate. I felt this would clear things up some for those who have been reading TAP since we started it up again. I also must say in his defense, if it was not for him, you would not be reading this today. I am not mad at him because i understand his point of view, i just don't like him trying to undermine my direction of TAP.

I have printed a letter someone sent in. It's really is funny in some ways since it can and can't be true. It just depends on how you look at it. If you want to reply you may. I will print the replies in the next issue. I mentioned this letter in 102 but didn't get to print it in 103. The story about the Perfect Wilson is rather faint. That was the best i could get it to come out. I had the option of either printing it like that or not printing it at all. So just be thankful you got to see it. If you have a story similiar send it in and i will print it.

In issue 103 there was an article on The Dictator. I don't really have much else to say. The articles were reprinted from Computer Underground Digest if you want to get the whole thing. I selected what i did because it had parts about him being on the bbs and having been at summercon. I will let you draw your own conclusion about feds being on boards. I think it is wrong, but who am i?

Deadline for the next issue is March 21st, with mailing around the 28th.

==========

-=-

So you want to know about Amerika? by Predat0r

-=-

I have decided to spread my subversive roots into another publication. Since i have taken over TAP Magazine i have turned it around and expanded it, but i feel limited reporting on computer hackers and phone phreaks and their ways. I want to share the things average americans feel, think, dream and do. I want to make this seperate from TAP since changing the format would mean losing what has already been built. What will Amerika be about? Well that is pretty easy. I want to publish stories relating to anything american. These can be fiction, non-fiction, science fiction, cyberpunk, poems or reviews of television, audio, video, or other publications (books etc). I want everyone to be able to express themselves without having to hold any feelings back. I want to share with others what people really think. How their minds work and what they think about. There is no set format it is going to be open to anything a writer feels like sending in. I will send out an issue to everyone who has an article published. This will be your chance to tell your side of the story, so off your talents and have your story read by many people. I will take either pro or con sides to anything and try and give equal space to each. If i get swamped with cons and one pro thats the way it will be.

Submissions must be typed and readable, or printed from a printer after being typed on some form of word processor. You may also send in your articles on either 5 1/4" 360k or 3 1/2" 720k ibm diskettes in ascii format. I will not take long hand unless you have no way of gaining access to the above means, and i do not guarantee i will have time to type them up for publication.

Basic format will be as follows. Editors notes, general information, articles and submissions from writers, and the following will be paid in advance to fund the magazines printing costs. Personal ads, for sale, trade or barter ads, and ads for other magazines which wish to advertise through Amerika. Pictures for personals can be used.

I will take any artwork including cartoon strips and drawings of original material. So if you are talented in art you may use the pages as well. Just make sure they are photocopy ready.

Send all entries to,

Amerika
C/O TAP Magazine
Post Office Box 20264
Louisville, Kentucky 40250-0264

If you have any questions you may also write to that address. Be sure to include a return address i can read. Print neatly please!

Or if you have a personal computer and modem handy you can call 502-499-8933 and follow the directions to access the bulletin board.

THE DNA BOX

Hacking Cellular Phones
by
The Outlaw Telecommandos

P A R T T H R E E

Previous DNA files discussed the possibility of using Japanese handheld HAM radios and personal computers, or tape recorders to hack Cellular Phone codes, and possible uses for investment & business info obtained by hacking executive and corporate phone calls, and investment info services, as well as approaches to modifying the Cellular Phones themselves for use as hacking tools and pirate communication devices.

Here using and modifying UHF-band radio scanners to hack and monitor Cellular and Mobile telephone systems will be dealt with.

Radio Shack, Uniden, and several other manufacturers make scanners for use by amateur radio hobbyists. Most of these will intercept mobile radiotelephone calls without modification by tuning in frequencies in the 156 MHz and 475 MHz regions. Most of these scanners have line-level audio outputs that can feed a tape recorder or demodulator/tone decoder chip which can then interface directly to a computer for analyzing codes. Mobile phones use a tone-pulse dialing protocol that should be simple to decode and emulate using standard handheld ham radio gear. You can almost count the dialing beeps without any special equipment. Phone channels are easy to find: they usually broadcast a standard busy signal or an idle tone (a fixed audio sine wave) when waiting for the next call. You will also hear conversations, ringing, and mobile phone operators on these channels.

Here's a partial list of frequencies used by mobile phones:
(frequencies in MHz)

152.51	154.57	152.66	152.69	152.72	152.78	154.54		
475.45	475.475	475.55	475.6	475.8	475.825	475.85	475.9	476.05

As you can see, many of the frequencies are spaced 30KHz or 25KHz apart, so there are probably more channels in the gaps at those intervals.

These frequencies were gathered in a few minutes of casual listening using an unmodified Radio Shack Pro-2021 scanner in search mode.

SCANNING CELLULAR FREQUENCIES:

Hobby scanners capable of monitoring Cellular Phones are prohibited in the US. To save money on the production line, many international scanner manufacturers make only one kind of scanning chip which they use in both US and foreign models. These chips are capable of scanning in the 800MHz range but this feature is diabled by grounding certain pins in the US models.
Often restoring Cellular scanning functions is merely a matter of cutting a circuit trace or removing a single diode from a scanner's printed circuit board.

For instance, removing diode 513 from a Radio Shack Pro-2004 Scanner will enable the 870MHz Cellular range. Installing diode 510 will increase the number of scanning channels from 300 to 400. Installing diode 514 will increase the scanning rate from 16 to 20 channels per second.
These are located on the printed circuit board labeled PC-3.

e Uniden Bearcat 200/205XLT can be modified for Cellular scanning
cutting or removing the 10K-ohm resisitor located on the printed circuit
ove the letters "DEN" on the microprocessor chip labeled "UNIDEN UC-1147".

The Regency Electronics MX7000 Scanner reportedly scans Cellular Phones without modification.

An additional scanner rumored to be modifiable is the Realistic Pro-32.

Another source of useful radio gear are "Export Only" manufacturers. One of these is currently rumored to be offering a handheld cellular phone that does it's own routing and has an operating radius of 160 kilometers!

CELLULAR PHONE FREQUENCIES:
Here are the frequency range assignments for Cellular Telephones:

Repeater Input (Phone transmissions) 825.03 - 844.98 Megahertz
Repeater Output (Tower transmissions) 870.03 - 889.98 Megahertz

There are 666 Channels. Phones transmit 45 MHz below the corresponding Tower channel. The channels are spaced every 30 KHz.

CORDLESS PHONE FREQUENCIES:
It's also possible to hack the popular cordless phones. These use the 49MHz band used by baby monitors and toy FM walkie talkies. Scanners can be used to monitor these without modification, and FM handheld transceivers will allow 2-way hacking of these frequencies, which some may find amusing.

Channel	Handset Transmit	Base Transmit	
1	49.67	46.61	(frequencies in Megahertz)
2	49.845	46.63	
3	49.86	46.67	
4	49.77	46.71	
5	49.875	46.73	
6	49.83	46.77	
7	49.89	46.83	
8	49.93	46.87	
9	49.99	46.93	
10	49.97	46.97	

Business Update:
As of January 1989 there are legal maneuvers going on to lift the ban on portable phones by traders at the NY Stock Exchange.

Another Point of View:
What the life of a phreakers is really like.

Who Are They?

Generally the range in age from 12-30. They are generally white males. They are frustrated members of the middle class. Because their parents abused them, and they never had everything they asked for, they have grown bitter. They go through life looking for a free ride anywhere they can find one. They are the slugs that you find on the underside of society. They grow up and move out into rooms above old stores in the cities. The cockroach infested homes, which generally run for $35 per month, have a sink and a toilet. The sink runs with rusty water. The window also faces out towards another brick wall. The phreaker has a bed in one corner and a computer in the other.
They awake in the morning and head to the 7-Eleven. They work there until 4:00 p.m. They then return home to finish off a stale bag of Cheetohs for dinner. They go to their greasy keyboard and begin phreaking. They collect information about the phone companies and computer networks. They, like pack-rats, store everything they can get their grubby little hands on. They continue until 2:00 a.m. Going to bed they dream of meeting a real girl someday that is not a relative. This is a portrait of your average phreaker. They are disillusioned with a society that does not cater to their needs. In turn, they choose to destroy it.

Modifications
To
Radio Shack PRO-2004

Scanner

These mods are extracts detailed in the following articles:

a) POPULAR COMMUNICATIONS AUG 87, PP 18-20

b) MONITORING TIMES OCT 87, P 53

c) MONITORING TIMES DEC 87, P 60

I would suggest that you obtain the back issues and read through the letters and articles. Also that you subscribe to the magazines. They supply a lot of interesting scanner information as well as useful frequency lists. Also Radio Shack sells a technical manual on all their electronic equipment, which contains maintenance and calibration procedures, as well as schematics.

Preliminaries:

First, treat the radio as if it were CMOS. That is make sure you take precautions concerning static charges. Second, unplug the radio from the antenna and AC power. Remove batteries. Take the radio out of the case by removing the 4 screws on the back. Carefully invert the radio. Locate a box-like sub-circuit. It's near the switch marked "restart". The sub-circuit should be marked PC-3. Carefully pry off the cover of the metal box. Inside there will be a 64 pin dip IC. This is the radio CPU. Be careful not to touch or short out any leads on the chip.

1) Restoring 870 MHz coverage.

Near the chip there will be a row of diodes marked D-502 to D-515. If D-513 is present, cut one lead, separate it so they will not touch, and 870 Mhz is restored. If D-513 is not there and you still do not have 870 coverage, then a little more work is in order. Locate the 9 pin connector "CN-501". Carefully remove it from the sub-circuit. Remove the screws holding PC-3 to the main chassis. Carefully invert the sub-circuit board (PC-3). Locate the lone component on that side of the board. If it is a diode, as it should be, then cut one lead and separate them as above. Re-install the sub-circuit with the screws on to the main chassis. Reconnect the 9 pin connector. Do NOT put the cover back on just yet.

2) Increasing from 300 to 400 channels

On the top of the sub-circuit board, locate the slot for D-513. Count backwards from there until you get to the space for D-510. Install a diode at D-510 in the same polarity as the rest of the diodes. You now have 400 channels instead of 300.

3) Increasing scanning speed to 20 channels per second

Now install a diode at D-514 and you have increased the scan speed to 20 channels/sec from 16 ch/sec.

4) Improving squelch operation

Carefully reassemble the metal box. Make sure everything else is as it should be. Invert the radio so it is right side up. Now, locate a sub-circuit box under the sloping front panel. It should have many alignment holes in the top. Pry the cover off very carefully. Locate IC-2 in the left side of the pc board. It should be marked IC-10420. Locate R-148, a 47 K ohm resistor between pins 12 and 13. Cut a lead of this resistor, But be sure to leave enough lead on both sides of the cut to solder to. Patch in a 100K ohm resistor. Make sure there are no solder balls or short circuits. Now your squelch will operate much better.

Again, I strongly suggest you obtain the above mentioned magazines for more details.

73
(Ham Radio Callsign Deleted)

PS, install the metal cover and the radio back in the case.

Addresses:

Popular Communications
76 N Broadway
Hicksville, NY. 11801

Monitoring Times
140 Dog Branch Rd
P.O. Box 98
Brasstown, NC 28902

The above edited text received on usenet, a network of unix(tm) computers. This modification voids your warranty. If you don't understand electronics, you have no business behind the front panel. Take it to someone who guarantees their work. It will be much cheaper that way.

********** Track Layouts **********

This is off the top of my head, but is 99% there. Also I'll ignore some obsolete stuff.

The physical layout of the cards are standard. The LOGICAL makeup varies from institution to institution. There are some generally followed layouts, but not mandatory.

There are actually up to three tracks on a card.

Track 1 was designed for airline use. It contains your name and usually your account number. This is the track that is used when the ATM greets you by name. There are some glitches in how things are ordered so occasionally you do get "Greetings Bill Smith Dr." but such is life. This track is also used with the new airline auto check in (PSA, American, etc)

Track 3 is the "OFF-LINE" ATM track. It contains such nifty information as your daily limit, limit left, last access, account number, and expiration date. (And usually anything I describe in track 2). The ATM itself could have the ability to rewrite this track to update information.

Track 2 is the main operational track for online use. The first thing on track to is the PRIMARY ACCOUNT NUMBER (PAN). This is pretty standard for all cards, though no guarantee. Some additional info might be on the card such as expiration date. One interesting item is the PIN offset. When an ATM verifies a PIN locally, it usually uses an encryption scheme involving the PAN and a secret KEY. This gives you a "NATURAL PIN" (i.e. when they mail you your pin, this is how it got generated.) If you want to select your own PIN, they would put the PIN OFFSET in the clear on the card. Just do modulo 10 arithmetic on the Natural PIN plus the offset, and you have the selected PIN. YOUR PIN IS NEVER IN THE CLEAR ON YOUR CARD. Knowing the PIN OFFSET will not give you the PIN. This will required the SECRET KEY.

Hope that answers your question

********** Deposits at ATMs **********

Deposits on ATM:

Various banks have various systems. As an example, at CITIbank a deposit was made to a specific account. Your account was updated with a MEMO update, i.e. it would show up on your balance. However it did not become AVAILABLE funds until it was verified by a teller. On the envelope was Customer ID number, the envelope number and the Entered dollar amount, the branch # and the Machine #.

There was also a selection for OTHER PAYMENTS. This allowed you to dump any deposit into the ATM.

What are you assured then when you deposit to an ATM ?

1) You have a banking RECORD (not a reciept at Citibank). If you have this record, there is a VERY high percentage that you deposited something at that ATM.

2) Some banks have ways of crediting your deposit RIGHT NOW. This could be done by a balance in another account (i.e. a long term C.D. or a line of credit.) That way they can get you if

you lied.

********** ATM Splitting a Card in half **********

I've worked with about 75% of the types of machines on the market and NONE of them split a card in half upon swallow. However, some NETWORKS have a policy of slicing a card to avoid security problems.

Trusting an ATM. Intresting you should bring this up, I'm just brusing up a paper describing a REAL situation where your card and PIN are in the clear. This involves a customer using a bank that is part of a network. All the information was available to folks in DP, if they put in some efforts to get it.

Mis-Implementation of an ATM PIN security system

1. Synopsis

In an EFT (Electronic Funds Transfer) network, a single node which does not implement the proper security can have effects throughout the network. In this paper, the author describes an example of how security features were ignored, never-implemented, and/or incorrectly designed. The human factors involved in the final implementation are explored by showing several major vulnerabilites caused by a Savings and Loan and a regional EFT network's lack of vigilance in installing an EFT network node. While using an EFT system as an example, the concepts can be extrapolated into the implementation of other secured systems.

2. Background

A small Savings and Loan was setting up a small (10 to 16 ATMs) proprietary Automatic Teller Machine (ATM) network. This network was then intended to link up to a regional network. The manufacturer of the institution's online banking processor sent an on-site programmer to develop the required interfaces.

An ATM network consists of three main parts. The first is the ATM itself. An ATM can have a range of intelligence. In this case the ATM was able to decode a PIN (Personal Identification Number) using an institution supplied DES (Data Encryption Standard) key. It was then required to send a request for funds to the host where it would receive authorization.

The second portion of the network is the ATM controller. The controller monitors the transaction, and routes the message to the authorization processor. The controller would also generally monitor the physical devices and statuses of the ATM.

The third portion of the network is the authorization system. In this case customers of the local institution would have the transaction authorized on the same processor. Customers from foreign (i.e. one that does not belong to the institution that runs the ATM) institutions would be authorized by the regional network. Authorization could be from a run-up file which maintains establishes a limit on withdrawals for a given account during a given period. A better method is authorization direct from the institution which issued the card.

3. Security

The system has a two component key system to allow access to the network by the customer. The first is the physical ATM card which has a magnetic stripe. The magnetic stripe contains account information. The second component is the Personal Identification Number (PIN). The PIN is hand entered by the customer into the ATM at transaction time. Given these two parts, the network will assume that the user is the appropriate customer and allow the transaction to proceed.

The Magnetic stripe is in the clear and may be assume to be reproducible using various methods, thus the PIN is crucial security.

Security PIN security

3.1. PIN security

3.1.1. PIN key validation method

PINs can be linked up to a particular card in a number of ways. One method puts the PIN into a central data base in a one-way encrypted format. When a PIN is presented, it would be encrypted against the format in the data base. This method requires a method of encrypting the PIN given at the ATM, until it can be verified at the central site. Problems can also occur if the institution wants to move the PIN data base to another processor, especially from a different computer vendor.

Another method is to take information on the card, combine it with an institution PIN encryption key (PIN key) and use that to generate the PIN. The institution in question used the PIN key method. This allows the customer to be verified at the ATM itself and no transmission of the PIN is required. The risk of the system is the PIN key must be maintained under the tightest of security.

The PIN key is used to generate the natural PIN. This is derived by taking the account number and using DES upon it with the PIN key. The resulting number then is decimialized by doing a lookup on a 16 digit decimalization table to convert the resulting hexadecimal digits to decimal digits. An ATM loaded with the appropriate PIN key can then validate a customer locally with no need to send PIN information to the network, thereby reducing the risk of compromise.

The PIN key requires the utmost security. Once the PIN key is known, any customer's ATM card, with corresponding PIN can be created given a customer account number. The ATM allows for the PIN to be entered at the ATM in two parts, thus allowing each of two bank officers to know only one half of the key. If desired, a terminal master key can be loaded and then the encrypted PIN key loaded from the network.

The decimalization table usually consists of 0 to 9 and 0 to 5, ("0" to "F" in hexadecimal where "F" = 15). The decimalization table can be put into any order, scrambling the digits and slowing down an attacker. (As a side note, it could be noted that using the "standard" table, the PIN digits are weighted to 0 through 5, each having a 1/8 chance of being the digit, while 6 through 9 has only a 1/16 chance.)

When handling a foreign card, (i.e. one that does not belong to the institution that runs the ATM), the PIN must be passed on to the network in encrypted form. First, however, it must be passed from the ATM to the ATM

you lied.

********** ATM Splitting a Card in half **********

I've worked with about 75% of the types of machines on the market and NONE of them split a card in half upon swallow. However, some NETWORKS have a policy of slicing a card to avoid security problems.

Trusting an ATM. Intresting you should bring this up, I'm just brusing up a paper describing a REAL situation where your card and PIN are in the clear. This involves a customer using a bank that is part of a network. All the information was available to folks in DP, if they put in some efforts to get it.

Mis-Implementation of an ATM PIN security system

1. Synopsis

In an EFT (Electronic Funds Transfer) network, a single node which does not implement the proper security can have effects throughout the network. In this paper, the author describes an example of how security features were ignored, never-implemented, and/or incorrectly designed. The human factors involved in the final implementation are explored by showing several major vulnerabilites caused by a Savings and Loan and a regional EFT network's lack of vigilance in installing an EFT network node. While using an EFT system as an example, the concepts can be extrapolated into the implementation of other secured systems.

2. Background

A small Savings and Loan was setting up a small (10 to 16 ATMs) proprietary Automatic Teller Machine (ATM) network. This network was then intended to link up to a regional network. The manufacturer of the institution's online banking processor sent an on-site programmer to develop the required interfaces.

An ATM network consists of three main parts. The first is the ATM itself. An ATM can have a range of intelligence. In this case the ATM was able to decode a PIN (Personal Identification Number) using an institution supplied DES (Data Encryption Standard) key. It was then required to send a request for funds to the host where it would receive authorization.

The second portion of the network is the ATM controller. The controller monitors the transaction, and routes the message to the authorization processor. The controller would also generally monitor the physical devices and statuses of the ATM.

The third portion of the network is the authorization system. In this case customers of the local institution would have the transaction authorized on the same processor. Customers from foreign (i.e. one that does not belong to the institution that runs the ATM) institutions would be authorized by the regional network. Authorization could be from a run-up file which maintains establishes a limit on withdrawals for a given account during a given period. A better method is authorization direct from the institution which issued the card.

3. Security

The system has a two component key system to allow access to the network by the customer. The first is the physical ATM card which has a magnetic stripe. The magnetic stripe contains account information. The second component is the Personal Identification Number (PIN). The PIN is hand entered by the customer into the ATM at transaction time. Given these two parts, the network will assume that the user is the appropriate customer and allow the transaction to proceed.

The Magnetic stripe is in the clear and may be assume to be reproducible using various methods, thus the PIN is crucial security.

Security PIN security

3.1. PIN security

3.1.1. PIN key validation method

PINs can be linked up to a particular card in a number of ways. One method puts the PIN into a central data base in a one-way encrypted format. When a PIN is presented, it would be encrypted against the format in the data base. This method requires a method of encrypting the PIN given at the ATM, until it can be verified at the central site. Problems can also occur if the institution wants to move the PIN data base to another processor, especially from a different computer vendor.

Another method is to take information on the card, combine it with an institution PIN encryption key (PIN key) and use that to generate the PIN. The institution in question used the PIN key method. This allows the customer to be verified at the ATM itself and no transmission of the PIN is required. The risk of the system is the PIN key must be maintained under the tightest of security.

The PIN key is used to generate the natural PIN. This is derived by taking the account number and using DES upon it with the PIN key. The resulting number then is decimialized by doing a lookup on a 16 digit decimalization table to convert the resulting hexadecimal digits to decimal digits. An ATM loaded with the appropriate PIN key can then validate a customer locally with no need to send PIN information to the network, thereby reducing the risk of compromise.

The PIN key requires the utmost security. Once the PIN key is known, any customer's ATM card, with corresponding PIN can be created given a customer account number. The ATM allows for the PIN to be entered at the ATM in two parts, thus allowing each of two bank officers to know only one half of the key. If desired, a terminal master key can be loaded and then the encrypted PIN key loaded from the network.

The decimalization table usually consists of 0 to 9 and 0 to 5, ("0" to "F" in hexadecimal where "F" = 15). The decimalization table can be put into any order, scrambling the digits and slowing down an attacker. (As a side note, it could be noted that using the "standard" table, the PIN digits are weighted to 0 through 5, each having a 1/8 chance of being the digit, while 6 through 9 has only a 1/16 chance.)

When handling a foreign card, (i.e. one that does not belong to the institution that runs the ATM), the PIN must be passed on to the network in encrypted form. First, however, it must be passed from the ATM to the ATM

controller. This is accomplished by encrypting the PIN entered at the ATM using a communication key (communication key), The communication key is entered at the ATM much like the PIN key. In addition, it can be downloaded from the network. The PIN is decrypted at the controller and then reencrypted with the network's communication key.

Security
PIN security
PIN key validation method

Maintaining the the security of the foreign PIN is of critical importance. Given the foreign PIN along with the ATM card's magnetic image, the perpetrator has access to an account from any ATM on the network. This would make tracking of potential attackers quite difficult, since the ATM and the institution they extract funds from can be completely different from the institution where the information was gleaned.

Given that the encrypted PIN goes through normal communication processes, it could be logged on the normal I/O logs. Since it is subject to such logging, the PIN in any form should be denied from the logging function.

3.2. Security Violations

While the EFT network has potential to run in a secured mode given some of the precautions outlined above, the potential for abuse of security is quite easy. In the case of this system, security was compromised in a number of ways, each leading to the potential loss of funds, and to a loss of confidence in the EFT system itself.

3.2.1. Violations of the PIN key method

The two custodian system simply wasn't practical when ATMs were being installed all over the state. Two examples show this: When asked by the developer for the PIN key to be entered into a test ATM, there was first a massive search for the key, and then it was read to him over the phone. The PIN key was written on a scrap of paper which was not secured. This is the PIN key that all the customer PINs are based on, and which compromise should require the reissue of all PINs.)

The importance of a system to enter the PIN key by appropriate officers of the bank should not be overlooked. In practice the ATM installer might be the one asked to enter the keys into the machine. This indeed was demonstrated in this case where the ATM installer not only had the keys for the Savings and Loan, but also for other institutions in the area. This was kept in the high security area of the notebook in the installer's front pocket.

Having a Master key entered into the ATM by officers of the bank might add an additional layer of security to the system. The actual PIN key would then be loaded in encrypted form from the network. In the example above, if the installer was aware of the terminal master key, he would have to monitor the line to derive the actual PIN key.

The use of a downline encrypted key was never implemented, due to the potential complications and added cost of such a system. Even if it was, once violated, security can only be regained by a complete reissue of

customer PINs with the resulting confusion ensuing.

Security
Security Violations
Network validated PIN Security violations

3.2.2. Network validated PIN Security violations

Given the potential for untraced transactions, the maintenance of the foreign PINs security was extremely important. In the PIN key example above, any violation would directly affect the institution of the violators. This would limit the scope of an investigation, and enhance the chance of detection and apprehension. The violation of foreign PIN information has a much wider sphere of attack, with the corresponding lower chance of apprehension.

The communication key itself was never secured. In this case, the developer handed the key to the bank officers, to ensure the communication key didn't get misplaced as the PIN key did (This way he could recall it in case it got lost). Given the communication key, the security violation potential is simple enough. The programmer could simply tap the line between the ATM and the controller. This information could then generate a set of PIN and card image pairs. He would even have account balances.

Tapping the line would have been an effort, and worse yet he could get caught. However, having the I/O logs could serve the same purpose. While originally designed to obscure PIN information in the I/O logs, the feature was disabled due to problems caused by the regional network during testing. The I/O logs would be sent to the developer any time there was a problem with the ATM controller or the network interface.

The generation of PIN and card image pairs has a potential for even the most secured system on the network to be attacked by the lapse in security of a weaker node. Neither the communication key, nor the PIN should ever be available in the clear. This requires special hardware at the controller to store this information. In this case, the institution had no desire to install a secured box for storing key information. The communication key was available in software, and the PIN was in the clear during the process of decrypting from the ATM and re-encrypting with the network key. Any programmer on the system with access to the controller could put in a log file to tap off the PINs at that point.

The largest failure of the system, though, was not a result of the items described above. The largest failure in the system was in the method of encrypting the PIN before going to the network. This is due to the failure of the network to have a secured key between sites. The PIN was to be encrypted with a network key. The network key was sent in encrypted form from the network to the ATM controller. However, the key to decrypt the network key was sent almost in the clear as part of the start-of-day sequence.

Any infiltrator monitoring the line would be able to get all key information by monitoring the start-of-day sequence, doing the trivial decryption of the communication key, and proceeding to gather card image and PIN pairs. The infiltrator could then generate cards and attack the system at his leisure.

Security
Security Violations
Network validated PIN Security violations

The network-ATM controller security failure is the most critical feature since it was defined by a regional network supporting many institutions. The network was supposedly in a better position to understand the security requirements.

4. The Human Factors in Security Violation

It is important the users of a system be appraised of the procedures for securing the system. They should understand the risks, and know what they are protecting. The bank officers in charge of the program had little experience with ATM systems. They were never fully indoctrinated in the consequences of a PIN key or communication key compromise. The officers showed great surprise when the developer was able to generate PINs for supplied test cards. Given the potential risk, nothing more was done to try to change the PIN key, even though, they were quite aware that the PIN key was in the developer's possession. They once even called the developer for the PIN key when they weren't able to find it.

The developer had a desire to maintain a smooth running system and cut down on the development time of an already over-budget project. Too much security, for example modifying I/O logs, could delay the isolation or repair of a problem.

The regional network was actually a marketing company who subcontracted out the data processing tasks. They failed to recognized the security problem of sending key information with extremely weak encryption. The keys were all but sent in the clear. There seemed to be a belief that the use of encryption in and of itself caused a network to be secured. The use of DES with an unsecured communication key gave the appearance of a secured link.

The lack of audits of the system, both in design and implementation was the final security defect which allowed the system to be compromised in so many ways. An example of the Savings and Loan's internal auditors failure to understand the problems or technology is when the auditors insisted that no contract developers would be allowed physically into the computer room. The fact was, access to the computer room was never required to perform any of the described violations.

5. Security Corrections

As in any system where security was required, the time to implement it is at the beginning. This requires the review of both implementation ormed to verify that the procedures are followed as described in the plan. Financing, scheduling and man power for such audits must be allocated so security issues can be addressed.

For this institution, the first step would have been to indoctrinate the

Security Corrections

banking officers of the risks in the ATM network, the vulnerabilites, and the security measures required.

Custodians of all keys should be well aware of their responsibilities for those keys. A fall back system of key recovery must be in place in case an officer is not available for key entry.

The cost of installing hardware encryption units at the host should be included in the cost of putting in the system. The host unit could generate down-line keys for both the PIN key and the communication key thus making it more difficult to derive these keys without collusion from at least three people.

A secured communications key should be established between the Network and the institution. This would allow for the exchange of working communication keys. This key should be changed with a reasonable frequency.

All these areas should be audited in both the system specification and implementation to make sure they are not being abridged in the name of expediency.

6. Summary

In this view of a single institution, a number of failures in the security system were shown. There was shown a definite failure to appreciate what was required in the way of security for PINs and keys used to derive PIN information. An avoidance of up front costs for security lead to potentially higher cost in the future. The key area was the lack of audits of the EFT system by both the institution and the network, causing potential loss to all institutions on the network.

6 WAYS TO FOIL A VOICE-MAIL HACKER

A little security can go a long way in protecting your voice-mail system. Take these simple precautions, and hackers will pass up your company s system in search of one that's easier to crack.

CHANGE YOUR PASSCODE FROM THE DEFAULT SETTING. Avoid using common or obvious combinations such as "1234," "1990," or your phone extension.

CHOOSE A PASSCODE THAT IS AT LEAST SIX DIGITS LONG. A six-digit passcode is 100 times harder to crack than a four-digit code.

DON'T CREATE UNASSIGNED MAILBOXES. Deactivate boxes that will be unattended for long periods of time.

DISABLE REMOTE-CONTROL ACCESS TO THE SYSTEM ACCOUNT. Otherwise, callers who break into the system can access system-management functions and create new mailboxes or change greetings.

MONITOR THE SYSTEM FREQUENTLY, and keep tabs on patterns of use. If a single mailbox receives 200 calls in one day, or if the volume of calls increases appreciably after hours, it could mean the system is under attack.

USE YOUR VOICE-MAIL SYSTEM'S AUTO-DISCONNECT FEATURE. Auto-disconnect will cut off anyone who fails to enter a passcode correctly after a certain number of tries.

SAFEGUARD YOUR SYSTEM'S TOLL-FREE PHONE NUMBER. Don't post the number in a conspicuous spot or publish it in a general phone directory.

BE DISCREET WHEN LEAVING VOICE-MAIL MESSAGES. Don't leave messages you wouldn't want anyone to overhear; instead, ask the person you're trying to reach to call you back.

-- WENDY TAYLOR

From: [Ham Call Sign Deleted](via Packet)
To: ALL @ ALLUS
Re:(B) Pro34 mod (detailed)

R:891001/0447z @:[Ham Call Sign Deleted] Hawthorne, NJ #:6635 Z:07506

Date: 01 Oct 89 02:30:17 UTC (Sun)
From: [UUCP Address Deleted] (Bob)
Message-ID: <5249@[Packet BBS Name Deleted]> (Wyckoff, NJ - 07481)
To: all@allbbs
Subject: Pro34 mod (detailed)

copied from UUCP:
Newsgroups: rec.ham-radio
Subject: PRO-34 Novice Notes (mods)
Disclaimer: I haven't tried this, proceed at your own risk [Call Sign Deleted].

"NOVICE NOTES" FOR PRO-34 MODIFICATIONS

1. Remove the 4 small phillips screws on the back of the unit
2. Remove the battery cover and battery holder from the case.
3. Remove the two knobs on the top of the case (Volume & Squelch)
4. The Case has some pressure fit points, These are at the bottom of the case and you need to be a bit careful in forcing the two halves of the case shell apart. Once you have the pressure fit points at the bottom released, angle up the bottom of the case until the battery separation wall is clear of the internal metal frame, and slide towards the top of the unit, place the back half of the shell aside.
5. Now you will see the RF board mounted to the metal support frame, The BNC (antenna) connector leads and the volume control power switch leads are soldered directly to the board. Carefully desolder these 4 connections.
6. At the bottom of the RF board there is a IF Can transformer that has a small wire as a grounding strap soldered directly to it. Desolder this as well.
7. There will be some wires from the volume control knob to the PC board that are socketed. Remove the plug from the RF board (needle nose pliers work)
8. There will also be a similar wire (small shielded) from the squelch control to the RF board which is also Socketed. Remove the plug from the RF board. (Again Needle Nose Pliers work good here)
9. Remove the 4 threaded stand-offs from the RF Board (these Hold the RF board to the internal metal frame and are where the screws that hold the back of the case on go.) Use a nut driver or Needle Nose Pliers.
10. Now there the RF board is mostly free. The only thing holding it in is the row of connector pins on its bottom side that plug into the logic board. You will need to pry this board up gently. Be warned that the bottom side of the RF board is just chock full of Very Small surface mounted components. So use something non-metallic and smooth to do the prying with.

11. Now that you have removed the RF board, place it along with the case shell back.
12. The Internal Metal support frame is now exposed. there are 3 small phillips screws holding the metal frame to the bottom Logic board (actually, these screws go through the logic board and into the front half of the case.) 2 of the screws are near the top, and 1 is at the bottom of the metal frame. remove these 3 screws.
13. There is a small socketed wire that leads from the small power pc board on the metal frame that goes under it and is plugged into the Logic board. Lift the metal frame up and remove the power plug from the PC board. Place the metal frame with the rest of your parts pile.
14. You are have the component side of the Logic board exposed now. There are 2 small phillips screws at the bottom of the PC board (where the Battery compartment WAS) Remove them.
15. Once you have the last 2 screw removed the Logic board is free. The speaker wires lead from the speaker to the logic board on the bottom side. These are soldered in but there is enough play in them to allow you to make the mods.
16. NOTE: The keyboard lock switch is a funky little piece of plastic with a sliding stainless metal contactor that is just wedged in between the front case and the logic board. Remove both the switch contacts and the plastic switch. (best know it now or loose them in the carpet)
17. On the component side of the PC board you will see lots of nifty surface mounted components, a fat little barrel capacitor (used for maintaining the channel freqs while you change the batteries.. and make modifications :) near the edge of the PC board you will see a couple of small diodes mounted vertically. These will be labeled on the PC board as D10 and D11, you will also see a place for another diode to be soldered in but was not installed at the factory.. this is D9.
18. You must now move diode D11 to the place where D9 is labeled. As you have probably noticed by now there is a tin cover over about 1/2rd of the PC boards solder side. The edge of the tin cover nearest the diodes has 2 metal tabs soldered to the P board. Desolder these 2 tabs and gently bend the metal cover way from the solder side of the PC board. This will expose the board enough to let you get your soldering iron in to where the diode leads are.
19. Desolder the D11 diode from the bottom while pulling it away from the board on the top of the board using needle nose pliers on the LEAD only.
20. Now heat up the D9 solder pads and insert the diode (the same way it was oriented in the D11 location)

You Have Completed the Mods for complete 800mhz band coverage and 66-88mhz band coverage.
LASTLY, Now that you have made the mods, you can use the warranty card to light the Bar-B-Q Grill with. :-)

The Charging Box

(c) Stinky Pig Productions

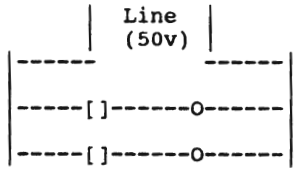
What it does:

The Charging Box is used to indicate when a call is being charged for and when it is not. Once installed, the box has two lights, a green and a red. Green means free and red shows that you are being stung by BT!

Components:

1 x green LED
1 x red LED
2 x short lengths of wire
1 x circuit board
2 x 10K ohm (1/4 watt) resistors
2 x small bulldog clips

Circuit Diagram:



Where [] is a resistor and O is an LED.
NB. IMPORTANT! One LED should have it's anode towards the resistor and the other should have it's cathode towards the resistor.

Connection:

Build that onto the board and connect the two points marked line to the wire, with the bulldog clips at the end. The box should now be connected to the line in parallel with the phone.

Operation:

When the line is opened (Ie. the phone lifted) the green LED will light (if the read one does then just reverse the polarity of the box). Dialling numbers (by pulse) will cause the green LED to flicker but while you are making free calls it should never go out and the red LED will not light. As soon as the exchange starts charging for your call, the green LED will go out and the red LED glow.

How it works:

As the LEDs are in opposite directions, only one can light depending on the polarity of the current supply. This is exploited when the exchange begins charging as the polarity of the line is reversed.

Total cost 2.20

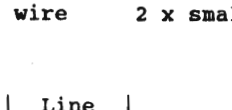
Extras -

1 blue coloured box (spray this pink to conceal purpose of device)
1 9v battery

Construction -

The device is very simple to construct and can be made small enough to fit onto a 10x24 veroboard.

Note: ZTX 300 Transistor



How the Device Works -

The three resistors and the capacitor set the frequency.
If the capacitor is 0.1uF then the resistor value can be calculated in the following way:

$$R = \frac{23000000}{\text{frequency}}$$

So, the resistor value for 2600hz would be:

$$R = \frac{23000000}{2600} = 8846.15 \text{ Ohms}$$

(this is no good, however because it must be more than 10K)

The frequency that the 4047B outputs is then amplified by the two transistors(a darlington pair) before being put through the loudspeaker.

Using the Device -

1) Dial a long-distance unobtainable number.
2) Hold the speaker against the phone microphone.
3) Send the 2280hz tone by holding the switch down on the device.
4) Pulse/Tone(exchange dependent)dial the exchange number.
5) Dial number to connect to.

NB: DO NOT CONNECT THIS DEVICE INDIRECTLY OR DIRECTLY TO ANY TELEPHONE NETWORK IN THE UK.