(>View: automatic teller machines
From ames!amdahl!nsc!voder!wlbr!gins Mon Jul 13 12:41:23 PDT

Article 479 of sci.crypt:

Path: ames!amdahl!nsc!voder!wlbr!gins

>From: gins@wlbr.UUCP (Fred Ginsburg)

Newsgroups: sci.crypt

Subject: Re: ATM secret codes

Summary: ATM stuff

 LONG...

Message-ID: <1038@wlbr.UUCP>

Organization: Eaton IMS, Westlake Village, CA

Lines: 445

A

In article <548@l.cc.purdue.edu>, roz@l.cc.purdue.edu (Vu Qui Hao-Nhien) writes:

> In article <127@ddsw1.UUCP> karl@ddsw1.UUCP (Karl Denninger) writes:

> >In article <192@sugar.UUCP>, karl@sugar.UUCP (Karl Lehenbauer) writes:

>

> The transactions done by ATM sometimes (not always) are kept by the

> machine until remove by human hands and fed to the bank's computer at

> its headquarters. Hence not much communication between ATM and the

> outside world.

> --

on computer security. Any questions, give a call (818-706-4146)

or send to {trwrb,ihnp4}!wlbr!gins

********** 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 suc@e603ty 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 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 and operational plans for the network. Audits should be performed 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.