Vulnerability and security issues in Auto teller machine transactions

NAVNEET SHARMA

Sr. Asstt. Professor Dept. of Computer Sc.
The IIS University, Jaipur, Rajasthan, India

E-Mail navneetsharma1977@gmail.com

Under the supervision of Dr. Vijay Singh Rathore
(Director Shri karni College, Jaipur, Rajasthan, India)

Abstract—In today's era of banking operation, identity theft, password protection is no longer adequate to guard your personal information, this paper will explain you the internal structure of ATM, processing of data in machine, data transmission, various security aspects. It will help you to understand the operational issues of auto teller machine, few levels of vulnerabilities of data transaction and security levels of data and encryption standard used in banking data security.

Keywords—auto teller machine, network, data encryption

Introduction:

Auto Teller Machines are a part of everyone's life. They ease the customer's to do financial operation outside the bank in a variety of places. Auto teller machine is an electronic unattended banking outlet, which allows customers to complete banking basic transactions without a direct branch interaction or a branch representative or teller. It is connected to a data system and related equipment and activated by a bank customer to obtain cash withdrawals and other banking services. It consist of computers with a keypad and screen to perform operations. to access Bank accounts it provided through telephone networking, a host processor, and a bank computer to verify data.

There are two types of ATM are card based and card less. A card based automated teller machine has a card reader to read a card (token), Keypad, a printer for receipts, an area for deposits, a money dispenser and a processor and A card less automated teller machine has a biometric device to receive biometric information about the customer, input device, a storage device including a database of customer information, processor, and money dispenser.

Functions of each unit of ATM:

Card reader:

Card reader is a device to identify particular account number. For this there is a magnetic stripe on the back of the ATM card is either swiped or pressed on the card reader. the card reader captures account information and passed on to the host processor. The host processor thus uses this data to get the information from the card holder’s bank.
Keypad – keypad is used for various inputs like pin number and to mention various actions to perform on machine. Once the card reader recognized the authenticity of the card, the machine asks for personal identification number (PIN), operations which you want to perform like withdrawal, balance enquiry, etc.

Display Screen – different operations instructions displays on the display screen for the user. All transaction information and the input from the user is displayed on the display screen. Each step of withdrawal is shown by the display screen.

Receipt printer – All the details regarding your withdrawal like the date and time and the amount withdrawn and also the balance amount in the bank is also shown in the receipt. Thus a paper receipt of the current transaction is obtained by the user.

Cash dispenser – This is the central system of the ATM machine. This is from where the required money is obtained. From this portion the person can collect the money.

Biometric device – It is a biometric device which is used to receive biometric information about the customer like fingerprint and other impression to identify the user.

Storage device – It is used to store a database of customer information, including stored biometric information. t

Processor - Processor is configured to receive the input signals from the input device, receive biometric information from the biometric device, and access the database of customer information in response to the input signals to obtain data about the customer identified by the customer identifier, biometric information for the customer. The processor then compares the received biometric information to the stored biometric information, and provides a message to the banking network provider confirming the customer's identity when the received biometric information matches the stored biometric information.

Block diagram of an ATM

The internal structure of an ATM is shown in figure 1. In this diagram there is a central processor which is connected with various input and output units. These are display unit, function keys, card reader, encrypted pin pad, printer, memory device, crypto processor and a modem. These devices are connected with bus. When a transaction is made, the details are inputted by the card
holder. This information is passed on to the central processor. The central processor checks these details with the authorized bank. If the details are correct, the requested cash by the card holder is taken with the help of an electronic fund from the customer’s bank account to the host processor’s account. After this function is carried out, the processor sends an approval code to the ATM machine so that the cash can be transferred from the vault.

**How Auto Teller Machine works:**

**Activation of Machine**

An automated teller machine (ATM) remains in stand-by mode until someone inserts the ATM card. There are three heads, namely, a magnetic stripe card reader, two three tracks, and one of them, read-only for the two heads, three heads can read and write, the second track a number of information stored by the second track to obtain the magnetic signal, after amplification, the decoder card number to obtain information the general reader read the card the data which is on a magnetic strip on the back of the card includes the bank's routing number, the user's bank account and their password. Once the card is entered, the machine reads the information from the magnetic strip and prompts the user to enter their password or "PIN" (personal identification number). If the PIN entered matches the PIN stored on the card, then user gains access to the ATM's other functions.

**Communication in a network**

Once card reader reads the information from the magnetic strip, using the bank's routing number, the ATM connects to the main host computer of the bank that issued the card via communication channel. Once connected, the ATM allows the user to perform various operations of banking. For example, the user wants to withdraw money, the request for the amount is sent to the bank that checks the amount against the amount in the account. If the amount requested is the same as or less than the amount in the bank, the withdrawal is approved, and the bank deducts the amount from the account. If the amount requested is more, the withdrawal is denied. For safe and secure data transmission in the network data communication data transfers in encrypted form. To secure transmission of confidential information like pin number, password etc. in the network, there are so many methods are used for encryption of information.

**Dispensing Money**

Once the ATM receives approval, it dispenses the specified amount of money through a slot in the machine. The money is held in a sealed container with a spring-loaded bottom to maintain pressure. Rubber wheels in contact with the top bill(s) roll, causing the money to be dispensed into a holding area until the correct amount is reached. Once the correct amount is counted out, the bills exit via the external slot to the user. The ATM then returns the card, prints a receipt and returns to standby mode.

**Security levels in auto teller machine:**

**User level security:**

**PIN Authentication**

This is the basic security measure used by all banks. It requires a 4 digit PIN number as credentials in order to access account on ATM functionality. This level can be divided into several levels of security depending on extending security levels of
data and bank. To increase the level of security PIN should be of 6 to 8 digits long.

Image/biometric

It is used as an additional level of user authentication. The image verification method consists of an image, when configuring the user account, account holder's information captured in the bank’s database like thumbprint or face image recognition. When we start functioning with ATM, it authenticates the account holder’s image with biometric input for authenticity of the user.

Network/system level security

Magnetic card readers to obtain card data:

The general reader, there are three heads: a magnetic stripe card reader, two: Three tracks, one of them, read-only for the two heads, three heads can read and write, second track a number of information stored by the second track to obtain the magnetic signal, after amplification, the decoder used to obtain information. This method has the advantage of safe, and reliable to obtain data from the card.

In the ATM machine the reader modules function is to determine the validity of bank cards, card number and other information will be sent into the host (ATMC side) and wait for the next step to deal with. Due to take into account the module and the general standard, the card reader module output signal using a common 485 or 422 or 232 serial port, and other means of communication, the way through the card reader module card number will be sent to the host (ATMC side). At the same time, separate the signal all the way into the ATM monitor host. Since the method does not involve ATM and the host (ATMC side) and other transaction data from the security point of view it is feasible, at the same time the introduction of universal means of communication, reliability and operability is also strong.

Data encryption:

To transfer data for validation in a network from ATM to host computer data send in an encrypted form so that any unauthorized user cannot access the secure information at the time of data communication in a public network.

Vulnerabilities over security in ATM transactions

1. In PIN card transactions, customers insert their card and enter their PIN into a PIN Entry Device (PED). The card sends its details to the PED. The PED also sends the customer's PIN to the card for verification. Both of these exchanges are unencrypted, and together contain enough information to create a fake card. Two of the most popular PEDs the Ingenico i3300 and Dione Xtreme, fail to adequately protect card details and PINs. The banking industry chose to deploy PIN cards that do not encrypt the data exchanged between the card and the PED during a transaction. By tapping these communications, fraudsters can obtain the PIN and create a magnetic strip version of the card to make ATM withdrawals. Fraudsters, with basic technical skills, can record this information and create fake cards which may be used to withdraw cash from ATMs.

To remove this type of vulnerability banking industries should use The DDA (Dynamic Data Authentication) cards allow the PIN to be encrypted and so preventing it from being intercepted. Banks could also block magnetic strip
transactions. They could also alter the copy of the magnetic strip stored on the chip, replacing it with an "iCVV compliant cards.

2. The Chip & PIN terminal can be opened, its internal hardware replaced, and that it can be re-assembled without external evidence. After replacing the new internal hardware, everything is under control of the fraudster: the card reader, the LCD display and the keypad. This means that the card reader can record information from the chip and display it on the screen. The data from the keypad, fraudster could allow to make cards with a fake magnetic stripe, which along with the PIN.

To protect this type of tampering with machine.The terminals do incorporate anti-tampering protection.

3. Relay Attacks: Eavesdropping attacks collect account and PIN data for use at a later date, but rely on the magnetic stripe fallback mode of operation, if the attackers are well-prepared, they can use the access to the customer's card and PIN in real-time: this is called a relay attack. Using this type of attack a fraudster can use GPRS to Transfer data to another terminal and can access account and perform fraud transaction from a bank to another terminal.

**Data encryption method for secure data communication in banking transactions in network:**

In auto teller machine for secure data communication, various data encryption methods are used. DES is the standard for data communication. DES (Data Encryption Standard) is the transformation of data to a form which is impossible to read without the appropriate knowledge or key. The Data Encryption Standard (DES) was developed to provide data security in network by an IBM team around 1974 and adopted as an international standard in 1977. 3DES is a revised variation of this standard due to the need for higher levels of security. all the banks are using this encryption standard for secure data communication in a public network.

There are different approaches to cryptography like public / secret key encryption and different algorithms are used for each type of system. 3DES is a cryptosystem, which can encrypt and decrypt data using a single secret key. 3DES “3DES” is as the name implies three times slower than regular DES but can be billions of times more secure if used properly. 3DES enjoys much wider use than DES because DES is so easy to break with today's rapidly advancing technology. 3DES was the answer to many of the shortcomings of DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. 3DES is an excellent and reliable choice for the security needs of highly sensitive information includes the future of PIN enable ATM transaction security. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right most) bit in each byte is a parity bit, and should be set
so that there are always an odd number of 1’s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for 3DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

REFERENCES
4. R. Sililiano, ATM Security threats Aug. 2010
5. www.scribd.com
6. www.circuitstoday.com