IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 01-06
www.iosrjournals.org

A study on Vulnerabilities of Automatic Teller Machine

[1]Minu C.M, [2]Sheema Madhusudhanan, [3]Prof. P. Jayakumar
[1]*Dept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India minu.rsch@gmail.com*
[2] *Dept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering, Kadayiruppu, Kerala, India sheemamadhu@gmail.com*
[3]*Professor, Dept. of CSE Sree Narayana Gurukulam College of Engineering, Kadayiruppu, Kerala, India nkartha@hotmail.com*

Abstract: Banking is basically about efficient service delivery. Customers can access their bank deposit or credit accounts by using an Automatic Teller Machine and make a variety of transactions. Automatic Teller Machines are a part of most of our lives. The next biggest application of security after government is in banking, and evolved to protect automatic teller machines (ATMs) from fraud. Vulnerabilities may result from bugs or design flaws in the system. A consumer becoming more dependent on ATMs and the proliferation of ATM debit cards, computer crime in this area is more likely to increase. This study is on types of ATM system vulnerabilities and security countermeasures provided currently including new efforts.
Key words : *ATM, vulnerability, security.*

I. Introduction

An automated teller machine or automatic teller machine also known as an automated banking machine is an electronic telecommunications device that enables the customers perform financial transactions, particularly cash withdrawal, without the need for a human cashier, clerk or bank teller. ATM like other technologies usually comes along with some limiting factors and individual problems. Numerous studies have shown that electronic payments have many benefits to users' convenience, securities. But on the darker side a number of customers have faced cheating and frauds through ATM. Vulnerability means to risks to which Automatic Teller Machines are open for misuse, abuse, damage and destructions by unauthorized person. Security issues to Automated Teller Machines means the exploitation of vulnerabilities.

II. Vulnerabilities In Atm Transactions

Automatic teller machine vulnerability mean weakness in the overall system which exploit the banking operation and allows an unauthorized user to have access to any other customers' account and perform financial operation using Automated teller machine for transacting from any other customers' account. In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance could directly or indirectly lead to the compromise of confidentiality, integrity, or availability of information or service anywhere on the network. Main three types of breaches are:

Confidentiality breach: it occurs on unauthorized read access.
Integrity breach: it occurs on creation, modification, or deletion of files.
Availability breach: it generates when denial of service.

2.1 Key Vulnerabilities

A recent study on a risk analysis of global ATM vulnerabilities narrowed the risks that happened on ATMs. Those risks down to three core focus areas:

A. Physical Vulnerability - the actual break-in of an ATM
B. Logical Vulnerability - protection from malware
C. Fraud - what we commonly known as skimming.

A. Physical Vulnerability

Physical Vulnerability is related to Automatic teller machine manufacturing defect or weakness that will help hackers to make physical changes in the manufacturing of machine. It may be some external attachment of external skimming devices to read the information and make a fake card or get the secure information using these external devices.

A Few Physical vulnerabilities are listed below:

- Card Skimming
- PIN Spying
- Pin interception
- Card Trapping/Fishing
- The Lebanese loop
- Dispenser False Fronts
- False ATM
- Partial Withdrawals
- Ram Raiding
- Robberies
- Safe cutting via frontal attacks etc

Card Skimming: In card skimming a fraud uses a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card. The information collected, copied onto another blank card's magnetic stripe is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder. Cards with magnetic strips are easy to clone with readily available and cheap card readers [1, 2]. Even though chip-based (EMV) cards are recently gaining popularity, cards still come with the magnetic strips, and it will be a while till all point-of-service devices and banks are upgraded to support only EMV cards. Unfortunately, such EMV cards are still vulnerable to cloning of the bank's certificate and relay attacks [3, 4].

PIN Spying: Spying PIN entry with hidden cameras while user entering his pin number on ATM center. There are lots of hidden cameras are available in market those are not even visible to our eyes.

PIN Interception: This is a process where after the user entered the PIN, info is captured in electronic format through an electronic data recorder. It can be done either inside the terminal or as the PIN is transmitted to host computer for online PIN check [5].

Card Trapping/Fishing: A criminal act where a card used in an ATM transaction is illegally captured by using fishing probes/hooks usually made by plastic ribbons or thin metal ribbons, inserted into the card reader throat and preventing the ejection and return of the card to the Customer[6].

The Lebanese loop: The Lebanese loop involves criminals inserting a card-capturing piece of plastic into the bank machine. When a victim inserts his card it becomes stuck inside the ATM. One of the fraudsters will often then appear and offer to help, watching the customer as he re-types his PIN. The victim then walks away assuming his card has been "swallowed" - leaving the thief free to recover it and, using the PIN he has just memorized, withdraw as much money as possible.

Ram Raiding: Criminals attempt to remove the ATM from its location, often by tying a chain to it and detaching it with a truck or other large vehicle. Ram raiding was the most successful method of attack and also the most frequently attempted attack, accounting for 45.4% of the attacks included in the study [7].

Dispenser False Fronts, False ATM, Partial Withdrawals, Robberies, Safe cutting via frontal attacks are same as the above mentioned attacks. They are common attacks which arise due to user's malpractices and misuse.

B. Logical Vulnerability/ Data Attacks

Logical Vulnerability relates to software weaknesses where a software attack can easily compromise the ATM, by the use of some virus attack or malware attack. Logical weaknesses are used to steal sensitive computer information and details of ATM cards. The information gathered is used for cloning a card i.e. for making a fake ATM card with all genuine information of the original ATM card.

Logical Vulnerabilities are listed below:

- Malware
- SQL injections

- Viruses
- PIN hacking
- Packet sniffing
- Jackpotting etc.

Malware: Cybercriminals have developed and implemented malware designed to withdraw cash directly from ATMs without compromising consumers' debit cards. The ATM malware allows criminals to identify the amount of money in each cash cassette and manipulate the machine to dispense it.

Security experts warn about a trio of malware threats that are designed to steal cash, online banking credentials as well as payment-card data from point-of-sale devices. GreenDispenser Malware, Shifu Banking Trojan, Neutrino Malware are the most recent malware threats to ATM [8].

GreenDispenser provides an attacker [with] the ability to walk up to an infected ATM and drain its cash vault. When installed, GreenDispenser may display an 'out of service' message on the ATM, but attackers who enter the correct PIN codes can then drain the ATM's cash vault and erase GreenDispenser using a deep-delete process, leaving little if any trace of how the ATM was robbed.[8] A crimeware toolkit malware Neutrino is also now targeting POS devices. It is designed to infect Windows systems via removable drives and network folders, and gives attackers the ability to use capture keystrokes and screenshots from infected systems, copy clipboard data, launch a remote shell, launch DDoS attacks, as well as steal data from POS device memory.

PIN hacking: PIN hacking means stealing the PIN. There is a method in which by using adaptive decimalisation tables and guesses, the maximum amount of information is learnt about the true PIN upon each guess [9]. A whole new family of attacks has recently been discovered on the application programming interfaces (APIs) used by security processors. The basic idea is that by presenting valid commands to the security processor, but in an unexpected sequence, it is possible to obtain results that break the security policy envisioned by its designer [10].

Jackpotting: "jackpotting" or exploiting automated teller machines is an attack to make ATM dispense cash without withdrawing it from a bank account using a bank card [11][12]

C. Fraud

Credit Card Fraud is a wide-ranging term for theft and fraud involving a payment card as a fraudulent source of funds in a transaction. This may leads to obtaining unauthorized funds from an account. Credit card fraud is also similar to identity theft. Skimming attacks will be more sophisticated and globally coordinated. "Flash attacks," which rely on coordinated, often international, efforts to simultaneously withdraw funds from multiple ATMs, are just the beginning [13].

Fraud techniques: There are many ways in which fraudsters execute a credit card fraud. As technology changes, so do the technology of fraudsters, and thus the way in which they go about carrying out fraudulent activities. Frauds can be broadly classified into three categories, i.e., traditional card related frauds, merchant related frauds and internet frauds[14]. The different types of methods for committing credit card frauds are described below:

Card related frauds
Application fraud

Application fraud occurs when a person fabricate an application to obtain a credit card.

Application fraud can be committed in three ways:
First one is *assumed identity*, where an individual illegally obtains personal information of another individual and opens accounts in his or her name, using partially legitimate information. Second type is *financial fraud*, where an individual provides incorrect information about his or her financial status to obtain credit card. Third category is Not-*received items (NRIs)* also called postal intercepts which occur when a debit or credit card is stolen from the postal service before it reaches its owner's destination.

Lost/ Stolen cards

A card is lost /stolen when a legitimate account holder receives a card and loses it or someone steals the card for criminal purposes. This type of fraud is in essence the easiest way for a fraudster to get hold of other individual's credit cards without investment in technology. It is also perhaps the hardest form of traditional credit card fraud to tackle.

Account takeover

This type of fraud occurs when a fraudster unjustifiably receive a valid customers' personal information. The victimizer takes control of a legitimate account by either providing the customer's account number or the card number. The fraudster then contacts the card issuer, masquerading as the genuine cardholder, to ask that mail be redirected to a new address. The fraudster reports card lost and asks for a replacement to be sent.

Fake and counterfeit cards

The creation of counterfeit cards, together with lost or stolen cards poses highest threat in credit card frauds. Fraudsters are constantly finding new and more innovative ways to create counterfeit cards. Some of the techniques used for creating false and counterfeit cards are listed below:

1. Erasing the magnetic strip: A fraudster can tamper an existing card that has been acquired illegally by erasing the metallic strip with a powerful electro-magnet. The fraudster then tampers with the details on the card so that they match the details of a valid card, which they may have attained, e.g., from a stolen till roll. When the fraudster begins to use the card, the cashier will swipe the card through the terminal several times, before realizing that the metallic strip does not work. The cashier will then proceed to manually input the card details into the terminal. This form of fraud has high risk because the cashier will be looking at the card closely to read the numbers. The security of cryptography depends on transient secret used in the cryptographic operation. In any pure software implementation of cryptographic algorithms, the key to be used must be somewhere in the memory at certain time no matter how the key is derived or obtained.

2. Creating a fake card: A common man can create a fake card from scratch using sophisticated machines. This is the most common type of fraud. Readily available softwares are there to produce fake cards.

3. Altering card details: A fraudster can alter cards by either re-embossing them by applying heat and pressure to the information originally embossed on the card by a legitimate card manufacturer or by re-encoding them using computer software that encodes the magnetic stripe data on the card.

4. Skimming: Most cases of counterfeit fraud involve skimming, a process where genuine data on a card's magnetic stripe is electronically copied onto another. Skimming is fast emerging as the most popular form of credit card fraud. Employees/cashiers of business establishments have been found to carry pocket skimming devices, a battery-operated electronic magnetic stripe reader, with which they swipe customer's cards to get hold of customer's card details. The fraudster does this whilst the customer is waiting for the transaction to be validated through the card terminal. Skimming takes place unknown to the cardholder and is thus very difficult, if not impossible to trace. In other cases, the details obtained by skimming are used to carry out fraudulent card-not-present transactions by fraudsters.

5. White plastic: A white plastic is a card-size piece of plastic of any color that a fraudster creates and put stolen data onto the backside of these cards. These cards are then used for financial transaction.

Merchant related frauds

Merchant related frauds are initiated either by owners of the merchant establishment or their employees. The types of frauds initiated by merchants are described below:

Merchant collusion

This type of fraud occurs when merchant owners and/or their employees machinate to commit fraud using their customers' accounts and/or personal information.

Triangulation

The fraudster in this type of fraud handles from a web site. Items are offered at heavily discounted rates and are also shipped before payment. The fake site appears to be a legitimate auction or a traditional sales site. The customer while placing orders online provides information such as name, address and valid credit card details to the site. Once fraudsters receive these details, they order items from a legitimate site using stolen credit card details. The fraudster then goes on to purchase other goods using the credit card numbers of the customer. This process is designed to cause a great deal of initial confusion, and the fraudulent internet company in this manner can operate long enough to accumulate vast amount of goods purchased with stolen credit card numbers. A new form of malware abstraction analysis technique based on control and data-flow based program analysis techniques to extract semantic signatures of such malware that are resistant to polymorphic and metamorphic modification.

Internet related frauds

The Internet has provided an ideal ground for fraudsters to commit credit card fraud in an easy manner. Fraudsters have recently begun to operate on a truly transnational level. With the expansion of trans-border or 'global' social, economic and political spaces, the internet has become a New World market, capturing consumers from most countries around the world. The most commonly used techniques in internet fraud are described below:

Site cloning: Site cloning is where fraudsters clone an entire site or just the pages from which you place your order. Customers have no reason to believe they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are identical to those of the real site. The cloned or spoofed site will receive these details and send the customer a receipt of the transaction via email just as the real company would. The consumer suspects nothing, whilst the fraudsters have all the details they need to commit credit card fraud. *False merchant sites:* These sites often offer the customer an extremely cheap service. The site requests a customer's complete credit card details such as name and address in return for access to the content of the site. Most of these sites claim to be free, but require a valid credit card number to verify an individual's age. These sites are set up to accumulate as many credit card numbers as possible. The sites themselves never charge individuals for the services they provide. The sites are usually part of a larger criminal network that either uses the details it collects to raise revenues or sells valid credit card details to small fraudsters.

Credit card generators: Credit card number generators are computer programs that generate valid credit card numbers and expiry dates. These generators work by generating lists of credit card account numbers from a single account number. The software works by using the mathematical Luhn algorithm that card issuers use to generate other valid card number combinations. The generators allow users to illegally generate as many numbers as the user desires, in the form of credit card formats, whether it be American Express, Visa or MasterCard.

III. Conclusion

This study contains a wide a summary of about vulnerability analysis on Automated teller machine operations, covering different types of vulnerabilities exist in Automated teller machines system, its related security issues.

Recommendations:

The followings recommendations are considered to be acceptable in the improvement and enhance the security of Automated teller machine and their users with several vulnerabilities and attacks. Automated teller machine should be more vulnerable from the physical attacks and therefore more protection may be needed form the physical security. There should be more security required for user's authentication and authorization as the single pin verification is not sufficient, it may be guess or trapped by the hackers. There should be dual verification bio-metric and pin to enhance the physical security. There should be high cryptographic securities included in data transmission for Automated teller machine networks as the communication lines may be hacked by expert hackers and they can trapped the encrypted data with some efforts. More anti skimming devices should be added by the manufacturers of Automated teller machine to protect the Automated teller machine with skimmers. Several anti-tempering sensors i.e. (thermal sensors, vibration sensors and smoke sensors) devices should be added in Automated teller machine from the manufacturers. Additionally there are new types of

authentication methods are coming in current days like card less transaction in which without a debit or credit card user can do transaction either by using wearable device or by using Smartphone [15].

References

[1] S. Schaible, "How thieves clone your credit cards," Online at http: //www.wfla.com/story/26074193/credit-cards-cloned, Jul 2014, wFLA News Report.
[2] J. Kegley, "Financial crimes: Credit card 'cloning' is a growing form of identity theft," Online at http://www.kentucky.com/2012/06/24/ 2236535/financial-crimes-credit-card-cloning.html, Jun 2012
[3] R. Anderson and S. J. Murdoch, "Emv: Why payment systems fail," Communications of the ACM, vol. 57, no. 6, pp. 24–28,Jun2014.[Online].Available: http://doi.acm.org/10.1145/2602321
[4] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks." in Proceedings USENIX Security Symposium, 2007, pp. 87–102.
[5] Christof Kier, Gerald Madlmayr, Alexander Nawratil, Michael Schafferer, Christian Schanes, Thomas Grechenig, "Mobile Payment Fraud: A practical view on the Technical Architecture and Starting Points for Forensic Analysis of new attack scenarios," *Proceedings of the International Conference on IT Security Incident Management & IT Forensics*, DOI 10.1109, pp. 68 - 76, May 2015.
[6] Online at http://securens.in/pdfs/KnowledgeCenter/5_ATM Fraud and Security.pdf
[7] SSMMAGAZINE " Ram Riding: The Biggest Threat to ATM Security" http://www.securitysolutionsmagazine.biz/2012/06/21/ram-raiding-the-biggest-threat-to-atm-security/, JUNE 21, 2012, Security Solutions Magazine.
[8] online at http://www.bankinfosecurity.in/malware-targets-bank-customers-atms-a-8551
[9] Dr. S.Sasidhar Babu," Exposing transient secrets and detecting malware variants using control and data flow analysis", international journal of computer engineering & Technology, Volume 5, Issue 12, December (2014), pp. 31-36,
[10] Mike Bond, Ross Anderson, "API-Level Attack on Embedded Systems", May 2001
[11] Goodin, Dan "Armed with exploits, ATM hacker hits the jackpot". The Register. Retrieved 7 August 2013
[12] Franzen, Carl "Barnaby Jack Ingeniously Hacks ATMs at Black Hat [VIDEO]". Aol News. Retrieved 7 August 2013
[13] B. Krebs, "Would you have spotted the fraud?" Online at http: //krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/, Jan 2010, krebs on Security, In-depth security news and investigation.
[14] T. P. Bhatla, V. Prabhu, and A. Dua, "Understanding credit card frauds," Cards business review, vol. 1, no. 6, 2003.
[15] Rasib Khan, Ragib Hasan, and Jinfang Xu, "SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices," Proceedings of 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, April 3 2015, pp. 41 – 50.
[16] Mike Bond and Piotr Zielinski, "Decimalisation Table Attacks for PIN Cracking" United Kingdom