Volume 3, No. 3, March 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

# ANALYSIS OF DIFFERENT VULNERABILITIES IN AUTO TELLER MACHINE TRANSACTIONS

Navneet Sharma[*1] and Dr.Vijay Singh Rathore[2]
Research scholer Suresh Gyan Vihar University, Jaipur, Rajasthan, India
navneetsharma1977@gmail.com[*1]
Director Shri karni College, Jaipur, Rajasthan, India
vijaydiamond@gmail.com[2]

***Abstract***— In today's scenario of banking operations, user identity protection, password protection is no longer safe to guard your personal information, in this paper we will try to explain different types of vulnerabilities and loose points which are attempted at the time of financial operations and generates fraud transactions due to fake entries and fake cards which makes the ATM vulnerable. Here we are presenting an analysis of few vulnerabilities over Auto Teller machine transactions. These vulnerabilities are categories in hardware vulnerabilities, software vulnerabilities, communication vulnerabilities and operational vulnerabilities. here we will discuss few types of vulnerabilities which makes the banking system unsecure and it results fake transactions over banking operations. Few vulnerabilities which we will cover in this paper are stand in time, skimming, Lebanese loop, pin entry vulnerabilities, etc.

***Keywords***—auto teller machine, vulnerability, skimming, stand in time, pin entry.

## 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. Mostly ATM uses the single entry customer identity verification using pin entry. if somebody gets your pin number and your card details then he can easily access your account and gets the fund using ATM and withdraw money from the ATM. In this paper we are presenting few vulnerabilities which makes an ATM vulnerable for ATM transactions.

## ANALYSIS OF VULNERABILITIES IN AUTO TELLER MACHINE

### *PIN card transactions Vulnerability:*

Mostly token (card) based transactions works on PIN (Personal Identification Number) verification . When the Customers insert their card and enter their PIN into a PIN Entry Device (PED)on ATM . there is a magnetic strip on the card which holds the information about the card holder. the card sends this information to the PED. The PED also sends the customer's PIN to the card for verification. Both of these exchanges are unencrypted and unsecure, and together contain enough information to create a fake card . Unfortunately the magnetic stripe information is simple to copy and counterfeit. As a result thieves have focused on methods of collecting this information. 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.

### *Hardware tempering Vulnerability:*

There are some weak points in designing of ATM terminals. The Chip & PIN terminal can be opened, its internal hardware can be 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.

***Skimming :***ATM skimming is now common in most parts of the world that have a mature network of ATMs, self-service terminals and point of sale (POS) terminals that accept magnetic stripe based credit cards and debit cards. Most bank ATM security issues and ATM fraud issues involving ATM skimming are the result of criminals attaching an ATM skimmer to the ATM card reader slot. Europe has historically been one of the most targeted geographies for ATM skimming attacks, although the world-wide spread of such ATM skimming fraud has been, and continues to be significant. ATM Card Skimming is a method used by criminals to capture data from the magnetic stripe on the back of an ATM card. Skimmer is a devices designed to look like and replace an ATM's card insertion slot. When an unsuspecting ATM user swipes his or her credit card through the fake dummy slot, the

skimmer makes a digital copy of the ATM's magnetic strip, making it easy for thieves to use a victim's credit card as they please. However, a new twist on this scam not only copies the credit card information, but also captures PIN numbers. Here are few skimming devices displayed bellow which are used for skimming

The skimming device being installed onto the card reader

Figure 1: skimming device installed at card reader slot

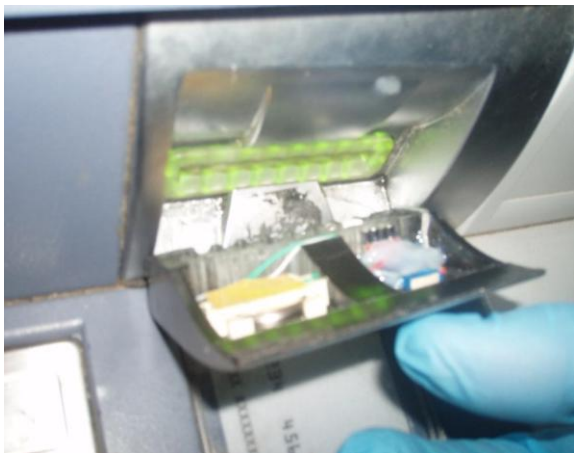

Figure 2: shows the internal view of skimming card reader

Here is custom-made skimmer kit displayed in figure 1,2,3,4 consists of two main parts: The upper portion (fig.1,2) is a molded device that fits over the card entry slot and is able to read and record the information stored on the card's magnetic stripe. The second component (fig. 3,4) is a PIN capture device that is essentially a dummy metal plate which look- like a PIN entry pad designed to rest direct on top of the actual PIN pad, so that any key presses will be both sent to the real ATM PIN pad and recorded by the fraudulent PIN pad .

Figure 3: skimming device for pinpad

Figure 4: skimming device for pinpad

***Lebanese Loop****:* this is a type of scame or type of vulnerability in which thieves insert clear plastic sleeves into the machine's card slot fitted with a loop of tape, wire, or strong thread over an ATM card reader. This allows a card to be inserted and read by the ATM, but not returned.When an unsuspecting customer inserts his or her card and enters their PIN, a message instructing the user to reenter the PIN is displayed because the machine cannot read the card's magnetic strip.After several unsuccessful attempts to reenter the PIN, the user finds that he or she cannot remove their card and, in many cases, leaves the machine mistakenly believing that the machine has malfunctioned and retained their card.In reality, the thief, posing as another customer feigning aggravation over the malfunctioning machine, was able to memorize the user's PIN following the unsuccessful entries, before leaving the area. After user leave, the thief removes the plastic sleeve containing the user's card, reinserts the card without the sleeve, enters the user's password and make transactions from the ATM.

**OPERATIONAL VULNERABILITY:**

***Stand in time:*** in this type of vulnerability ATM behavior can change during stand in time where the bank cash dispensing network is unable to access the database that contains account information (possibly the database maintenance). In order to give customers access to cash, customer may allow withdrawing cash up to a certain amount, but may exceed amount which is more than in exist account. It may result in fraud.

***Network vulnerability attacks against ATMs :***

ATMs communicate with the banking systems through a network connection are mostly using private networks and proprietary network protocols but more often these connections now using the Internet and using standard network protocols. Fraudsters or hackers can use some computer programs (malware) to attack the ATM and retrieve the control or gain access through a software or computer flaw. Once they have gained access to the ATM, they install software that collects card information and PINs. An ATM that has been compromised is not physically recognizable from one that has not and often users will be unaware of this type of fraud by which all the transactional information can accessed by the hackers.

## CONCLUSION

An ATM is more convenient to make cash transaction outside the bank premises Behind the friendly appearance of the Automatic Teller Machines, it provides secure banking transaction outside the bank. with possible security majors there are few weakness in atm transections and these vulnerabilities give a chance to hackers or fraudsters to make a attack on atm in a network to capture secure information and make fake transactions .in this paper we mentioned a comparative analysis of few vulnerabilities of ATM to prevent the secure data and atm transaction .

## REFERENCES

[1]. www.zdnet.co.uk/.../security.../phishing-attacks-highlight-banks-weaknesses-39211852

[2]. http://news.cnet.com/Phishers-cash-in-on-ATM-cards/2100-7349_3-5815141.html april, 2011

[3]. http://www.uml-diagrams.org/composite-structure-examples.html

[4]. http://www.hostfrontier.com/attachments/019_Skimmer%20presentation%20v1%20230109%20ppt%201%20.pdf

[5]. www.gartner.com/it/page.jsp?id=492168

[6]. http://www.enisa.europa.eu. ATM crime *Overview of the European situation and golden rules on how to avoid it*

[7]. http://www.ehow.com

[8]. www.wikipedia.org

### Short Bio Data for the Author

 Navneet Sharma (MCA, M. Phil. (Comp. Sc.), Ph.D (Pursuing) Sr. Asstt. Professor the IIS University Jaipur

 Dr. Vijay Singh Rathore (Ph. D, M. Tech. MCA, MBA) Director Shree Karni College, Jaipur

 