ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 10 , October 2015

A Survey on Secure PIN Authentication for ATM Transactions

V.Varalakshmi

P.G. Student, Department of Computer Engineering, IFET College of Engineering, Villupuram,Tamilnadu,India

ABSTRACT: Automated teller machine is very popular and most efficient ways for transaction of money. It perform financial transactions mostly cash withdrawal. It reduces the work load of banks as it is fully automated. Currently, Personal Identification Number(PIN) is used for security in ATMs and authentication is provided to the Users by entering the personal identification number (PIN).These PIN numbers can be hacked easily through specific fraudulent activities and it can be observed by human or device attackers. This paper describes aboutattacks on pin entry and secureATM Transactionsmethods used to reducephysical and electronic theft in ATMs.

KEYWORDS: personal identification number; Skimming Attack; Pin Authentication; shoulder surfing attack.

I. INTRODUCTION

Nowadays many unauthorized access, threats and theft takes place in ATM machines. Currently PIN numbers are used for security in ATMs. The crime rates are also increased with fleeting time and will never fall as attackers are efficient enough with all detailed criminal knowledge collected with them. The service provider must promote a stable security of user data for customer satisfaction. The goal is to protect ATM from theft using counter measures for security. As the ATM related security are public and published in newspaper and internet. So the security measures applied are known to both the regulator and attacker. Nowadays we use 4-Digit PIN code for safety and security for money deposition and transaction.

We believe that the money we deposit will be safe as the PIN code is secret and the card we use is safe with us. But in real the PIN numbers can be hacked easily through specific fraudulent activities and it can be observed by human or device attackers. The attackers now are technically knowledgeable they have every idea about the usage of the user. At first, the attacker will try hacking the 4-PIN code using finger prints plated in the number box. Then the hacker tries hacking the bar code of the card using the detector and a duplicate card of the user is framed for theft. Through this method the thief can withdraw our money without the regulators knowledge and initiate theft without any doubt. So, theSecure-PIN-Authentication methods are used to overcome this problem andthis work describes about attacks on pin entry and secure ATM Transactions methods.

II. ATTACKS ON PIN ENTRY

A. Shoulder Surfing Attack

In a shoulder-surfing attack (SSA), the attacker detects the logon procedure by looking over the user's shoulder, and tries to recover that user's PIN. The SSA may be done directly through the human eyes or by using any electronic devices such as fixing a skimmer device or mini cameras at ATMs.

B.Skimming Attack

A device that reads and stores magnetic stripe information when a card is swiped. An attacker can fixing a skimmer over the card slot of an ATM and store customers' credit information without their knowledge. Later, this information can be retrieved and used to make duplicates of the original cards

C.Eavesdropping Attack

In Eavesdropping attack, the Eavesdropper secretly listening to another person's conversation. In this attack the Eavesdropper secretly observing the users pin entry.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 10 , October 2015

D. Guessing Attack

In a guessing attack, the attacker guesses a user's PIN and inputs it to pass the test. The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or robotic approach. For example, a typical ATM permits three trials.

III. REVIEW OF LITERATURE

Mr. S.Kumaresan, Mr. G.Dinesh Kumar, Mrs. S.Radhika proposed shuffled Automated Teller Machine keypad method and they develop Bluetooth application [1]

The Pin entry can be observed by human or device attackers. To overcome this problem, they proposed shuffled Automated Teller Machine keypad which shows the shuffled numbers in the Liquid Crystal Display keypad which confuses person who standing near you to guess the password. Another one is to develop the Bluetooth application between the user and ATM counter for communicating a password through the wireless medium.Two methods are,
Shuffling keypad: To implement the keypad by capacitive touch based screen which changes the number display for each different user. The random number is generated by using LFSR (Linear Feedback Shift Register) one of the techniques to generate the shuffled numbers in a display [1]. LFSR is shift register whose input bit is a linear function of its earlier state. The linear functions of single bits are XOR and inverse- XOR.
Wireless Password Transfer: The mobile based security level is developed by creating the mobile application as Bluetooth which is used only by the ATM counters [1]. In the same way the ATM counter has individual Bluetooth which is used to exchange the data between the ATM database and user passwords.

AbdulrahmanAlhothaily, ArwaAlrawais, Xiuzhen Cheng, RongfangBie proposed a new cardholder verification method [2]

Security plays a crucial role in payment systems; however, some implementations of payment card security trust on weak cardholder verification methods, such as card and a signature, or use the card without having any cardholder verification process at all. To overcome this problem, they introduce a novel cardholder verification method that provides a high level of security for payment card systems.This method using a multi-possession factor authentication with a distance bounding technique, which prevents many different security attacks. So, this method gives the user the flexibility to add one or more extra devices and select the suitable security level and this technique trust on one or more personal RFID devices such as smart watches, smart phones, rings, necklaces, and bracelets

Mun-Kyu Lee have proposed the Black and White (BW) Method [3]

Where the regular numeric keypad is colored at random, half of the keys in black and the other half in white, which is called as BW technique. A user who knows the correct PIN digit can answer its color by pressing the separate color key.The basic BW method is expected to resist a human shoulder surfing attack. But if the selected halves were memorized or written on a paper for mconsecutive rounds and recalled to derive their Grouping Patterns, the shoulder surfer could recognize a single digit of the PIN.

A.D. Luca, E. von Zezschwitz, L. Pichler, and H. Hussmann presented a system using fake cursors [4]

To hide password entry on on-screen keyboards. The objective of the fake cursor is, adding overhead to the input to make it hard to monitor. The authors suggest several concurrent cursors that move in the exact same way to quickly reach objects on big screen spaces. In this system, only one cursor performs the actual input while the other cursors act as distraction for an attacker. That is, they do not move in line with the genuine cursor. Since the fake cursors move differently from the active cursor, users can identify it while attackers have problems to do so.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 10 , October 2015

Hong Guo, Bo Jin proposed [5]

Magnetic stripe cards are widely used by many different administrations to provide both convenience and security. These types of cards are often trusted on identification and personal authentication. However, they are not designed to withstand attacks that use the sophisticated technologies available today. For instance, skimming takes advantages of the fact that the digital content of a magnetic stripe card can be copied with perfection. The goal of this paper is to introduce the range of devices available for manipulating magnetic stripe card data

Sujith B proposed [6]

Nowadays investigation is going on in the field of crime detection and avoidance in the ATM. So the idea of designing and implementation of security for ATM project are born from the observation of our real life incidents happening around us. Over the past three periods consumers have come to depend on and trust the ATM to conveniently meet their banking needs. The suspicious object's visual properties so that it can be exactly segmented from videos. After analyzing its subsequent motion features, different abnormal events like Crimes and robbery can be effectively detected through videos. The proposed method will uses multiple object detection method and event recognition techniques of computer vision.

TABLE 1: Secure-Pin-Authentication Methods

S.NO	TITLE	METHOD
1	Design of Secured ATM by Wireless Password Transfer and Shuffling Keypad	Shuffling keypad -Linear Feedback Shift RegisterWireless Password Transfer- Bluetooth
2	A novel verification method for payment card systems	RFID Technology
3	Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PINEntry	Black and White(BW) Method
4	Using fake cursors to secure on-screen password entry	Fake cursor method
5	Forensic Analysis of Skimming Devices for Credit Fraud Detection	Magnetic stripe cards
6	Crime Detection and Avoidance in ATM: A New Framework	Object detection method

IV. ANALYSIS

ATM authentication using PIN-based entry is highly susceptible to shoulder-surfing and Skimming attacks. To overcome this problem, authors suggested Secure-Pin-Authentication methods [1, 2, 3, 4, 5]. But these methods also have some problems due to the skimming attacks. Because, the attacker has installed a card skimming device on the ATM machine to get hold of the user's card information. Such devices fit at the card slot on ATM machines and record the card information.

V. CONSTRUCTION OF PROPOSED SYSTEM

Theft of the ATM machines has been increased widely. By using the existed technologies, ATM machines are not safe in order to provide proper security for cash. To overcome this problem, the proposed work describe about Wireless authentication method using Wi-Fitechnology. In this technology, we use our own wireless devices (Laptop,Smartphone,Tab) for secure ATM Transactions. So, this Wireless authentication methodprovides a security to the PIN entry process from shoulder-surfing and Skimming attacks.

VI. CONCLUSION

Currently, Personal Identification Number(PIN) is used for security in ATMs and authentication is provided to the Users by entering the personal identification number (PIN). These PIN numbers can be hacked easily through specific

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 10 , October 2015

fraudulent activities and it can be observed by human or device attackers. So, this project describes about attacks on pin entry and secure ATM Transactions methods used to reduce physical and electronic theft in ATMs.

REFERENCES

[1]. Mr. S.Kumaresan, Mr. G.Dinesh Kumar, Mrs. S.Radhika, "Design of Secured ATM by Wireless Password Transfer and Shuffling Keypad", In IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems,978-1-4799-6818-3/15/$31.00, 2015 .

[2]. AbdulrahmanAlhothaily, ArwaAlrawais, Xiuzhen Cheng, RongfangBie, "A novel verification method for payment card systems", In Springer-Verlag London,October 2015, Volume 19, Issue 7, pp 1145-1156,October 2015.

[3]. Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PINEntry", In IEEE Transactions On Information Forensics And Security,VOL. 9, NO. 4, pp. 1556-6013,APRIL 2014.

[4].A. D. Luca, E. von Zezschwitz, L. Pichler, and H. Hussmann, "Using fake cursors to secure on-screen password entry", in Proc. CHI, pp. 2399–2402,2013.

[5]. Hong Guo, Bo Jin, "Forensic Analysis of Skimming Devices for Credit Fraud Detection",2nd IEEE International Conference onInformationand Financial Engineering (ICIFE), pp. 542 – 546,2010.

[6]. Sujith B, "Crime Detection and Avoidance in ATM: A New Framework",International Journal of Computer Science and Information Technologies, 2014.

[7]. Schneier B, "Applied Cryptography", John Wiley and Sons Inc., 1999

[8].B.Krebs, "Would you have spotted the fraud?" Online at http: //krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/, Krebson Security, In-depth security news and investigation,Jan 2010.

[9]. Banking:Personal Identification Number (Pin) Management And Security Part 1: Basic Principles And Requirements For Online Pin Handling In Atm And Pos Systems, Clause 5.4 Packaging Considerations, Iso 9564-1:2002, 2002.

[10]. V. Roth, K. Richter, And R. Freidinger, "A Pin-Entry Method Resilient Against Shoulder Surfing", In Proc. Acm Conf. Comput. Commun Security, Pp. 236– 245,2004.

[11]. Michael S. Scott, "Robbery at Automated Teller Machines", Guide No.8, 2001

[12]. Heli Snellman, "Automated Teller Machine network market structure and cash sage", ISBN 952-462-318-8, 2006.