

A review on security and reporting mechanisms for coerced cash withdrawal from ATM

Madhu Sharma¹, Vijay Singh Rathore²

¹Research Scholar, Suresh Gyan Vihar University, Jaipur

²Director and Professor, Sri Karni College, Jaipur

Abstract: With the increase in usage of ATM and the enhancement in technical strengths of the entire system including security aspects, the destructive aspects also came into existence in parallel. The ATM owners are worried for the logical and physical security of ATM, just after its implementation and usage. The entire security system demands the support of the customers and as well as the police services, for safe transactions through ATM. Customer is required to follow all the safety guidelines issued in favor of secure ATM usage and the police is required to be alert and active with a direct or indirect strict vigilance at ATM points. But still with all such strong security measures, a great number of logical and physical security attacks are being reported in almost every country of the world. In this paper, we have reviewed the existing security mechanisms for a duress or coerced cash withdrawal from ATM along with a brief discussion on various types of logical or physical attacks on ATM's security system.

Keywords: Automated Teller Machine(ATM), Personal Identification Number (PIN), Data Encryption Standard (DES), Triple DES, Message Authentication Code (MAC), Partial MAC, Global Positioning Systems (GPS), Intelligent Banknote Neutralization Systems (IBNS), Plofkraak, Transaction Acceptance Password (TAP), Safe Mode Alarm Reporting Technique (SMART).

I. INTRODUCTION

Over time, people have become dependent on indirect cash transaction facilities like internet banking, online transfer through credit or debit cards or machines like Automated Teller Machines. With the increase in demand and availing of such services, various types of frauds, logical or physical attacks are also increasing day by day. The challenge of finding efficient security mechanisms is upheld by many inventors and thus as its result, we do have a number of security mechanisms with their successful implementation.

As per the growing security problems relevant to Personal Identification Number (PIN) and card frauds of ATM, new authentication and security mechanisms are required to be introduced with the stronger support of infrastructure including both software and hardware updation to enhance performance [1]. Till today a number of attacks over ATM's security system, have been reported and a number of counter measure have been implemented successfully, but still the intensity of attack and its type is changing with the increase in criminal activities with the support of technical and non-technical measures. The crimes and attacks challenges the existing security measures and thus compels inventors to update the countermeasures to stop the growing number of ATM attacks.

With the increase in cases of indirect robbery or duress or coerced cash withdrawals, there is need of more effective implementations in this direction [2], [3]. Thus in this paper, we have discussed on the security measures available or have been invented for forced cash withdrawal by the ATM card holders under pressure or on indirect gun-point. An introduction to various types of attacks relevant to ATM has been discussed in section II of this paper, a review on various inventions for coerced or duress cash withdrawal from ATM has been discussed in section III and section IV concludes the paper.

II. ATM ATTACKS AND SECURITY MEASURES

ATM, being a rich repository of cash at public places, has greater chances of being attacked by the thieves and robbers. Also the customers who go for withdrawal are insecure before or after cash withdrawal from their own accounts. ATM has a great scope for the various types of attacks and cracks, until it is not secured logically as well as physically.

(A) SOFTWARE OR LOGICAL SECURITY ATTACKS

The security of ATM transactions is dependent on the integrity of the entire software security system including cryptoprocessor, encryption schemes implemented on ATM like Data Encryption Standard (DES), Triple DES, Message Authentication Code (MAC), Partial MAC etc. Security measures like alarming to police services on reverse entry of PIN in case of forced cash withdrawal, authentication on the basis of finger and palm vein patterns, iris and facial recognition technologies associated to avoid fraud cases due to attached fake keypads or card reader, Installation of alarm and sensor to prevent unauthorized entry in ATM area, CCTVs, display of on-screen safety warnings, placement of convex mirrors above the display allowing the user to see what is happening behind them are also introduced for a safer and secure transaction through ATMs. Few other common frauds like card skimming which involves the implementation of a magnetic card reader just over the actual ATM's card slot, usage of a wireless camera or digital camera or a fake keypad to detect the user's Personal Identification Number could be controlled through the preventive measures like usage of smart cards instead of simple ATM card, from which card information cannot be copied or hacked.

(B) PHYSICAL ATTACKS

From the beginning years of installation of ATM, Ram-raiding is a very general type of attack on ATM, where criminals attempt to uproot the machine from their original place. Usage of anti-crime deterrents, like fixing of bollards surrounding an ATM, usage of heavier ATM containers, ink-strainers, emergency fogging system, Global Positioning Systems (GPS) etc. could prevent ATM ram-raids. Criminal activities like staff- robbing or theft from ATM could be prevented by Intelligent Banknote Neutralization Systems (IBNS), Plofkraak i.e. breaking-in of ATM chamber using explosives and gases, could be prevented by using gas sensors and neutralizers within or near the ATM cash chambers. Attacks like tunnel digging could be prevented by installing security sensors for sensing geographical changes, connected with police or security service providers. A robbery like coerced cash withdrawal, are sensitive cases that could be handled through systems like Safe Mode Alarm Reporting Technique (SMART) in ATMs [4].

III A REVIEW ON SECURITY MEASURES FOR COERCED CASH WITHDRAWAL

Intelligent Banknote Neutralisation Systems (IBNS) is one of the known security techniques to prevent crime and protect cash and people at ATM. INBS get activated at the time of unauthorized access to the ATM cash, by marking or staining the cash by red, purple or green ink and thus make cash unusable [5].

Iain R. F. Sime stated about the inclusion of a biometric recognition technique with some predictive technique for ATM, to help to detect or check any fraud or an abnormal transactional behavior, before moving for final transaction process [6].

Donald A. Barnett stated about the invention of a security system where an authenticated customer is enrolled along with his registration with the financial institution and issuance of transaction card and this system actively keep check and respond on emergency calls, theft and frauds [7].

Ronald K. Russikoff meant to recognize and provide solution for the coerced cash withdrawals using a computerized password verification system through the inclusion of an additional password, termed as Transaction Acceptance Passwords (TAPs) to be selected from the list of all the TAP's opted by user in past [8]. This TAP selection is done after the usual PIN entry on ATM display screen. A secret and "panic" TAP is triggered, if wrong TAP is opted and a silent alert signal is forwarded to the relevant banking authorities and security personnel [8].

Alan J. Eisenberg patented that the security is achieved by providing two Personal Identification Numbers from banking authorities, one for normal transaction and another for dealing emergency situations. If the emergency PIN is entered, a secret alarm is forwarded to the security personnel, along with the simulated transaction in front of the criminals, to avoid any hint of alarm to him [9].

James E. Winner stated about his patented emergency communication system to be introduced at ATM, for handling emergency or unauthorized access, by providing the facility of a number – 911, which has to be pressed by the user before the beginning of the transaction as well as after the end of the transaction in emergency situations like duress cash withdrawal. This 911 number triggers an alarm at the 911 emergency stations [10].

Michael Wayne Brown et. al. and Susann Marie Keohane et. al. presented their idea of handling duress or coerced transactions at level similar to the patent US 5354974 A [9], but the additional mechanism introduced by them includes the marking of bills with special ink which could be visualized under specific light and recording of serial number of bills of duress transaction along with signaling to the security personnel [11], [12].

Donald R. Crowell et. al. patented, a secret communication network system of ATM with host computer, introduced to handle emergency situations. The first emergency signal is requested from the ATM, which then forwarded to the host computer to find the financial account of the user system and the second signal from ATM user is then forwarded to the financial institution to freeze his account [13].

Hitoshi Kokumai et. al. in their invention stated the method for protecting secret information in a system for reporting an emergency in case of unauthorized access to secret information. In coerced situation, user triggers a predetermined alerting signal which is added and set at the time of setting password in advance, which then utilized to inform the security personnel on emergency [14], [15].

Kenneth J. Peters in his invention stated the involvement of the set of programmed units involving a processor, display, a key pad, and a cash dispenser slot with a memory unit, programmed to recognize a 'panic' code keyed in by a user under coerced situation. The system protects user through normal behavior and retaining the user's card with no cash dispense, after the generation of secret message to the security services [16].

Samuel H. Bosch et. al. in their invention introduced a cost-effective, currency dispenser and control system (CDCS), which includes the duress dispensation system that allows the CDCS to activate an alarm and a time-release system that effects a time-delayed dispensation and forwards the secret signals to the nearby security services during a robbery or coerced withdrawal [17].

Samuel H. Bosch et. al. in their patent US 8332321 B2 [18] added feature of remote CDCS and CDCS independent of a standard ATM electronic fund transfer (EFT) network to the basic mechanism introduced by them in US 7726557 B2 [17]. Pradal Gabriel introduced a special security system that involves silent alarm activation by a user performing transaction on ATM or similar device using a magnetic card by entering one of the already listed System Activation Code (SAC) into the device. The different SAC's are associated with different levels of security measures like sending of sound and video signals to the security service providers, sending of information about the geographic location of the transaction device and demographic data of the card owner and so on [19].

CONCLUSION

Here we have discussed on various types of attacks on ATM. We have seen the different measures to deal such attacks. We have reviewed the inventions related to the coerced cash withdrawal from ATM. We can conclude that still there is a need of system which could make the cash secure and catch the criminals with the customer's safety always on priority.

REFERENCES

- [1]. M. Langheinrich, H.Hussmann, Proceedings of the Sixth Symposium on Usable Privacy and Security, ACM New York, ISBN: 978-1-4503-0264-7 [Online] Available: <http://dl.acm.org/citation.cfm?id=1837131>.
- [2]. D Teitelbaum, "Violent Crime At ATM", The Business Lawyer, 1990 - JSTOR, Vol. 45, June 1990.
- [3]. Schreiber, Francis B., "ATM Crime & Security Newsletter, Vol. 2, No. 2" (1992). [Online], Available: <http://repository.stcloudstate.edu/atmcs/4>.
- [4]. Sharma M., Rathore V.S., "An Investigative Study on Physical Security and Reporting Mechanisms in ATM", OORJA International Journal of Management & IT, ISSN NO: 0974-7869, Volume 16,/No. 1, Jan-April 2014 (In Press).
- [5]. European Commission (2014, Apr 18). Public Awareness - Stained Banknotes [Online]. Available: <https://www.european-atm-security.eu/Stained%20Banknotes>.
- [6]. Iain R. F. Sime, "System and method for detecting user fraud in automated teller machine transactions", US 5386104 A, January, 31, 1995.
- [7]. Donald A. Barnett, "Security card and system for use thereof", US 6068184 A, May 30, 2000.
- [8]. Ronald K. Russikoff, "Computerized password verification system and method for ATM transactions", US 6871288 B2 Mar 22, 2005.
- [9]. Alan J. Eisenberg, "Automatic teller system and method of operating same", US 5354974 A, Oct 11, 1994.
- [10]. James E. Winner, Jr, "Emergency communication system for automatic teller machines", US 6055438 A, Apr 25, 2000.
- [11]. Michael Wayne Brown, Rabindranath Dutta, Michael A. Paolini, Newton James Smith, Jr., "Automatic teller system and method of marking illegally obtained cash", US6679422, Jan 20, 2004.
- [12]. Susann Marie Keohane et. al, "User configurable alerts for ATM transactions", US 7328839 B2, Feb 12, 2008.
- [13]. Donald R. Crowell, Kenneth Algiene, "Emergency services notification from an ATM systems and methods", US 7549574 B2, Jun 23, 2009.
- [14]. Hitoshi Kokumai, Ryuhei Masuno, Masayuki Kuriyama, "Method for protecting secret information in a system for reporting an emergency when secret information is accessed", US8577807, Nov 5, 2013.

- [15]. Hitoshi Kokumai, Masayuki Kuriyama, Ryohei Masuno, "Secret information recorded medium, secret information protection method, secret information protective storing method, and system for reporting emergency such as theft or confinement when secret information is accessed", EP1313027A1, May 21, 2003.
- [16]. Kenneth J. Peters, "Anti-theft system for self-service terminal", EP0822525A2, Feb 4, 1998.
- [17]. Samuel H. Bosch, Jonathan H. Bosch, "Currency dispense and control system with anti-theft features", US7726557, Jun 1, 2010.
- [18]. Samuel H. Bosch, Jonathan H. Bosch, "Remote currency dispensation systems and methods", US8332321, Dec 11, 2012.
- [19]. Pradal Gabriel Gustavo Ocana, "Security system and silent alarm activatable by a user", WO2001071674A1, Sep 27, 2001.

