A SURVEY ON SECURITY MEASURES IMPLEMENTED TO DETECT BURGLARY AT THE ATM

Arpitha B.R[1], Madhusudhan K.N[2], Ashwini.V[3], Dinesh Reddy[4]

[1]MTech Student, Department of electronics and communication, BMSCE, Bangalore, India
[2]Assistant Professor, Dept of ECE, BMSCE, Bangalore-19
[3]Assistant Professor, Dept of ECE, BMSCE, Bangalore-19
[4]Assistant Professor, Dept of ECE, BMSCE, Bangalore-19

Abstract

Automated Teller Machines (ATMs) are part of most of our lives which eases access to financial transactions without direct interaction with bank authorities, but ATM attacks are major problem which are however inevitable even though certain security measures are implemented. The current work deals with survey on preventive measures took to avoid ATM thefts. The preventive measures took to prevent ATM fraud are installing alarms and sensors, video surveillance, awareness and consumer education, and remote monitoring. In order to avoid ATM thefts in real-time and to be able to react in time, a fully automated system is desired.

Keywords**—***ATM, video surveillance, computer vision, sensors, logical attacks in ATM*

---***---

1. INTRODUCTION

Consumers have come to depend on and trust the ATM since from past three decades to efficiently meet their banking needs [1]. ATMs don't need the continuous human involvement for monitoring and are mostly located in public places where attacks are possible which tend to attract perpetrators [2].

Thieves have been developing new ways to steal the cash from ATM since its introduction in 1967 [2]. In the year 2007, 212,530 theft cases and 4,439 robbery cases are happened and in 2010, 269,410 theft and 4,409 robbery cases are happened. And also in year 2011, 270,109 of theft and 4,509 of robbing cases are happened. Among the crime for financial organization, the cases of theft and robber have very high proportion of over 90% and the crime for the ATM has been increased because the external ATM has been increased and it is always exposed to the crime [3]. ATM crimes are not only limited to theft of cash, but also attackers seek to obtain consumer's personal identification number (PIN). While these types of identity theft attacks take more effort to net cash for criminals, the results are – illegally obtaining money [2].

Survey by Retail Banking Research estimate more than 2.2 million ATMs are deployed across the world by 2013 and these figures outlook to exceed 3 million ATM deployments by 2016 [4]. So the occurrence of security threats increases as the number of ATMs in use increases, making the development of fraud prevention measures a high priority for financial institutions (FIs) and ATM manufacturers.

2. AUTOMATED TELLER MACHINE

The first of automated teller machine (ATM) that was put into use was in north London, United Kingdom, on 27 June 1967 by Barclays bank in Enfield Town [5]. The evolution of ATMs from Early ATMs (1970's – 1980's) where limited services like cash withdrawals (typically in fixed and limited amounts), account balances (DDA), traditional deposits via envelopes to present day Next-Gen ATMs (2013 – till date), to name few services - bill payments, Integrated multi-channel capabilities, on-demand services, EMV, NFC proves the advancement of technology in terms of functionality, accessibility, security. Even after such advancement in technology towards ATM, threats related to ATM theft are still occurring. The architecture of an ATM is shown below in figure 1 [6].

ATM consists of both hardware and software. The hardware typically consists of CPU, magnetic or chip reader, keypad, secure cryptoprocessor, display, function keys, vault (Safe), sensors and indicators. ATMs use 'off-the-shelf' operating systems for software functionality.

3. TYPES OF ATM THEFTS

ATM thefts can occur to hardware or software of the system. Security attacks for ATM are classified into 3 classes: card and currency fraud, logical attacks, and physical attacks.

3.1 Card and Currency Fraud

This type of fraud involves in both direct and indirect ways. The direct way is to steal cash from the ATM system whereas indirect attack is to use consumer data to establish forge cards illegally and obtaining cash from consumer's account through fake atonement. The ways of Card and Currency fraud can be done are by Skimming, Card trapping/fishing and Currency trapping/fishing [7].

Skimmer devices obtain consumer card information using the magnetic stripe on the back of ATM card. Card trapping and fishing try to steal card information when consumer inserts the card for transaction inside card reader. Cash trapping or fishing means to attempt to collect cash which is not intended to any consumer, which means obtaining money from the ATM illegally.

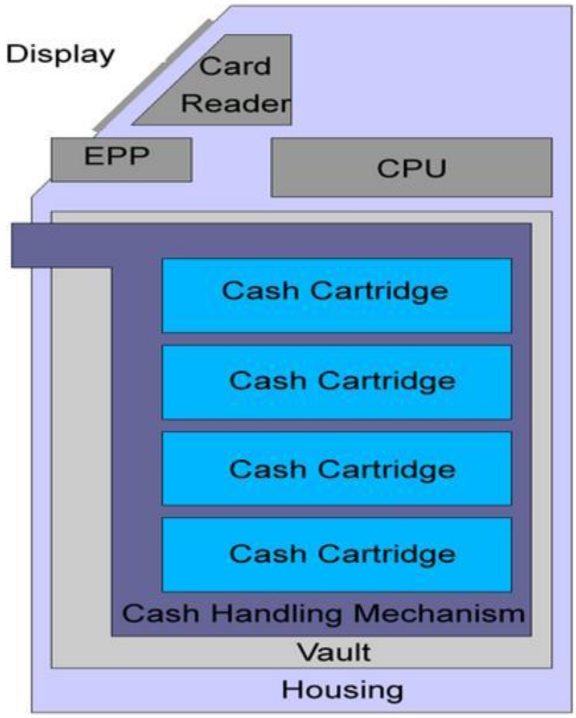

Fig. 1: ATM Architecture

3.2 Logical/Data Attacks

Logical attacks directly target to ATM’s software, communication systems and operating system which make these attacks most difficult to detect.

The Microsoft Windows® operating system has provided better, greater connectivity and interconnectivity of ATMs. The communication network which are connected via internet including ATMs, phone systems, branch systems and infrastructure are major targets of logical security threats. Viruses and malware are injected to ATMs operating system to violate integrity, confidentiality or authenticity of transaction related data [7].

3.3 Physical Attacks

Physical attacks are related to physically damaging the ATM by means of drilling, cutting etc. These attacks include any type of violation that damages components of the ATM in order to obtain cash. The main component for most physical attack includes vault, where the cash is stored in cash cartridges as shown in figure 1.

The methods of attacks include cutting/grinding with power saws or grinders, drilling with power drills, prying with wedges and crowbars, burning device such as thermal lance or any other use of explosives like dynamite, gas or homemade bombs.

4. SECURITY MEASURES TO AVOID ATM THEFTS

As the number of threats increasing from year to year, certain preventive measures have been implemented to prevent ATM thefts. The measures taken to avoid ATM thefts can be categorized into video surveillance, implementation of alarms and sensors, and remote monitoring.

4.1 Video Surveillance

Video surveillance is the basic and effective method implemented to create awareness and deter fraud attempts at the ATMs. This method is adopted by installing Closed Circuit Television (CCTV) Camera(s) in plain view or near the ATM [1]. Nowadays cameras can be easily integrated into upper top corners of ATMs and additional security can be achieved by installing extra site cameras inside and outside the premises. For this method, the cameras must monitor the premises continuously.

But continuous surveillance is a critical security issue in many states around the world. Remote sites offer particular challenges regarding maintenance issues so these can be solved with digital video recorders. Analyzing the video obtained from camera after any theft occurrence, cops can search/identify thief.

4.2 Alarms and Sensors

Sensors are integrated inside the ATM premises to detect any theft, and alarms are used to give the information to nearby people by whistling any type of sound. This type of method are implemented to detect the state of the ATMs vault door, whether the door is in open/closed condition, or used to monitor different parameters which indicate the attempt of robbery.

For example, Vibration sensors are used to detect any kind of piercing to ATMs vault [8]. Temperature sensor is used to identify the change in temperature while piercing with torch. Door sensor can be integrated to check the ATMs cabinet door status [1].

4.3 Remote Monitoring

Remote diagnostic services provide an automated means to manage and monitor our ATM network. Remote monitoring is helpful in delivering important messages with regard to any tampering with machine.

ATM terminal availability can be improved with the help of remote diagnostics, monitoring, and management with reduced risk. It develops expedition prevention of service technicians and facilitates a group of central support associates to manage and control from their PCs, mouse and keyboard operations of ATMs [1]. By developing fully fledged remote monitoring system, the current status messages from the ATM can be sent to central location on a pre-defined plan where these messages are acted upon. By using this facility, central support associates can manage ATM functionalities from remote location, this way the risk of service personnel working in ATM is minimized. Remote diagnostic services manage, control and track events at any ATM, to which the remote diagnostic services are available to route and document on every action.

4.4 Others

Ink Dye is type of ATM theft avoidance method where the cash is being sprayed with an ink on detection of any abnormalities with regard of ATM's hardware. Later the cash will not be useful for either bank authorities or robbers due to the ink stained currency notes. Anyhow this method didn't prove to be efficient since it is a loss to the Bank authorities itself [1].

Few people don't know how to conceal the information of their respective bank account details. The people without any awareness regarding the importance of bank account details provide account information on fraudulent calls asking for consumer bank details. These losses can be avoided by creating awareness and consumer education.

5. CONCLUSION

Even though with the advancement in security measures which are implemented to avoid robbery, somewhere or other ATM thefts are still occurring. As the technology is emerging to its new heights, logical/data attacks can be avoided with the efficient programming of software in terms of operating system. With the help of awareness and consumer education, card and currency thefts can be prevented to certain extent. The implementation of security measures including both video surveillance and alarms and sensors are proved to more efficient way to avoid ATM thefts. Remote monitoring can be helpful only when the group/authorities monitoring the ATMs are literate. Video surveillance with the addition alarms and sensors and also with the help of image processing techniques to detect human objects provides an efficient way to avoid ATM thefts.

REFERENCES

[1] Diebold, “ATM Fraud and Security White Paper”, 2003.

[2] Diebold, “ATM Fraud and Security”, 2012.

[3] P.Kannan, P.Meenakshi Vidya, “Design and Implementation of Security Based ATM theft Monitoring system”, Proceedings of “National Conference on Information Processing & Remote Computing Feb. 2014.

[4] “Global ATM Market and Forecasts to 2016.” Retail Banking Research. September 2011. Brochure Page 2.

[5] “Enfield's cash gift to the world". BBC London. 27 June 2007.

[6] Michael S. Scott, “Robbery at Automated Teller Machines”, Guide No.8, 2001

[7] From Mag Stripe to Malware: Card Security Risks in 2011. Aite Group. 2011.

[8] M.Ajaykumar and N.Bharth Kumar, “Anti-Theft ATM Machine Using Vibration Detection Sensor”, IJARCSSE, Volume 3, Issue 12, December 2013.