Chapter 7
Safeguarding of ATM

Srividhya Srinivasan
University of Madras, India

Priya Krishnamoorthy
SASTRA University, India

Raghuraman Koteeswaran
SASTRA University, India

ABSTRACT

An automated teller machine (ATM) is a kiosk that is used widely for money transactions across the globe. Several banking sectors have showed interest in deploying ATMs. The cash dispenser system manages the transaction services with less manual effort. When it comes to deploying an ATM, two methods are practiced: onsite ATM and offsite ATM. Safeguarding cash kept inside the ATM is a challenge. Researchers suggested several built-in security measures to secure the money in ATMs. Nevertheless, burglars still loot the money. Some widely used looting methods include card skimming, cash trapping, and phishing. So, it is time to give intelligence to the ATM itself to react to the situation. Proposed is a system that implements the idea of making machines to identify the situation and perform actions accordingly. This mechanism is not only about giving intelligence to it, but also a cost-effective one.

INTRODUCTION

In today's world ATM has become an inevitable part of human's life. All the developing countries are spending a lump sum of money in printing their currencies and to recycle it. Therefore, the world is changing towards cash-free transactions (Ray, 2015). Cash-free transactions can be done in various ways (PaymentWall Blog, 2015), among which plastic cards plays a vital role. According to (Sharad Raghavan.T.C.A, 2015; Hemali Chhapia, 2015), the cost of printing a currency note is much higher than that of its face value. Rather than spending a huge amount in printing and recycling notes, the cost of preparing plastic cards is considerably less. Hence in order to promote plastic cards as the primary mode of fund transfers, the banking sectors has introduced credit cards, debit cards, etc., throughout the world. Banks provide a number of card systems to facilitate and to attract the customers (BankBazaar.com). It

DOI: 10.4018/978-1-5225-7362-3.ch007

is estimated that the number of ATMs have been increasing every year (Diebold, Incorporated, 2012; Statistic Brain, 2015). Henceforth, security to safeguard ATM in all aspects has become an inevitable one. In this article, a hybrid model consists of both logical and physical ways of securing has been suggested.

BACKGROUND

An ATM is Kiosk machine which has been filled with cash of various denominations, where the person can withdraw money at any time, by using the plastic card. That plastic card has been given by the bank from where the person is having his/her account. That card has a magnetic stripe, a 16 digit card number, a Card Verification Value (CVV) and a 4 digit secret pin which helps the customer to withdraw the amount. Now-a-days, our Indian Government insists all the citizens must have an account in a bank and immediately a debit card has been given for it, thereby promoting cashless transactions. Hence it is mandatory to provide security features for an ATM (Diebold, Incorporated, 2012). Once a card has been issued, the banking sectors are insisted to place Automated Teller Machine (ATM) at various places throughout the country for the benefit of the people (BankBazaar.com). Many research works have been done in providing security for the kiosk machine. But, as per the Newton's Third law *For Every Action there is an equal and opposite reaction*, the more security researchers found, the more techniques were being followed by the robbers to steal the money from the ATM (Diebold, Incorporated, 2012). Kiosks placed within business areas are considerably safer and are less prone to get robbed (McGoey, 2015). Robberies are done by targeting free standing ATMs in the high ways (McGoey, 2015). Several techniques are used by robbers to steal cash, some of them are card/currency fraud, logical ways and hard ways of attacks (Diebold, Incorporated, 2012; Wild.O, 2015).

Card and currency fraud includes skimming, Transaction Reversal and card/currency trapping/phishing. In these techniques, the perpetrator would fix an extra device to an existing ATM and tries to grab the customer's confidential data thereby steals the money from their account.

In logical attack, the robbers attempt to grab the confidential data of the customers, in a smart way. In 2015, the malware attack is the most common logical attack, in which the perpetrator injects a virus called Tyupkin. The infected ATM will be then work under the control of intruder.

The physical attack is one, in which the robbers target the ATM and try to break it by drilling, cutting, and using fire exposures / explosives. Even, it includes pseudo ATM placement, removal of the ATM, smashing the ATM and many more. In some cases of logical and fraud methodology also, burgling is done by using partial breaking of the machine. Malware is a type of logical attack, in which a partial physical attack is implemented to open the top hat of ATM to inject the malware. Therefore, in any ways the ATM is disturbed by physical attack (Kaspersky).

Although several researches outcomes have been implemented to prevent and detect the ATM frauds, the physical attack on ATM is still increasing (E.A.S.T, 2016). The survey (SecureWorld, 2016) says the percentage of Physical Attacks on ATM is increased in a drastic way. According to European ATM Security Team (EAST), in the year of 2015 alone about €49m was stolen by hard breaking of around 2,657 ATMs (E.A.S.T, 2016). This is because; the main target of the looters is to grab the cash dispenser within a short duration.

There are several detection technologies and risk management technologies available that can expose attacks only after the money is gone (Peter Beardmore, 2016). So it is indeed not only to detect but also to safeguard the ATM from the intruders.