ATM- HACKING/ JACK POTTING – A CASE STUDY

M.Maheswari[*1], Shashikant Thube[*2], K.B. Jena[*3], Dr. P.Paul Ramesh[*4]

[1-4] *Central Forensic Science Laboratory, DFSS, MHA, GOI, Kolkata, West Bengal, India*

Abstract - *In the modern digital era, the extensive use technology has revolutionized all sectors like agriculture, banking, medicine, education, industries and so on. Digitization has brought out utmost ease and comfort in day-to-day life and has become inevitable part of the mankind. This has also led to misuse of technology through cyber crimes and cyber attacks. ATM hacking/ jackpotting is one such cyber crime where there is attack on an ATM vending machine to steal away the money. It is called ATM hacking as someone takes illegal control over the operation of ATM and Jackpotting as the ATM vending machine vulnerably dispenses all the cash to the attacker. In this paper, types of ATM hacking, vulnerabilities, and a case study in this regard is presented.*

Key Words: (ATM, ATM hack, ATM jackpotting, XFS, API, SPI, encryption etc)

1. INTRODUCTION

Prior to proceeding into the technicalities of how ATM attack is carried out, a brief understanding of how ATM works is required. In simple terms the ATM is just an extension of the bank and the ATM terminal is a sort of remote computer with a safe cash box attached to it. It is made up of the CPU (microprocessor) which carries out processing of information/data, visual display unit (VDU) which comprises of screen and keyboard which acts as an interface with the client/customer, secure crypto processors to encrypt and decrypt secure communications, network equipment, card reader and the currency box or vault which stores the cash, the cash dispenser which dispenses the cash and a receipt printer that produces hard copy of the transaction that have been affected [1].

ATMs are connected to network via ADSL or dial-up modem over a telephone line or direct leased line. All communications between the ATM and interbank network are encrypted for additional security. The computer usually runs on Windows, in a special embedded version designed specifically for ATM use. Only administrators have access to Windows; other users should not have such access. To do its job, the application must communicate with ATM peripherals: get card information from the card reader, obtain user input from the keyboard, and send commands to the cash dispenser. This communication takes place using XFS (extensions for financial services), a standard for simplifying and centralizing equipment control. With XFS, a hardware manager makes an API (application programming interfaces) available to all Windows applications and forwards requests to devices. Commands to each XFS-connected device are sent via the corresponding service provider (device driver). The hardware manager translates API functions to SPI (service provider interfaces) functions and forwards the result to the service providers. Each ATM vendor implements XFS in their own way[2].

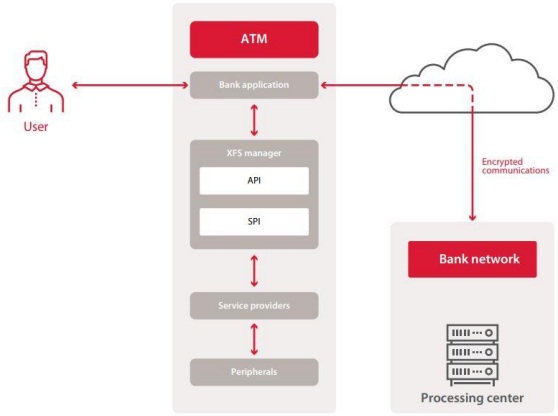

Fig -1: Interaction between ATM components [2].

2. HOW ATM IS ATTACKED:

ATM attacks traditionally started with the physical attacks on ATM machines wherein the hardware of the vault is broken using gas cutters and other type of equipments. The physical attacks involved lot of risks compared to the Malware attacks. Logical attacks or Malware / software-based attacks are now widely prevalent and depending on the vulnerabilities and security limitations, the heist is carried out effortlessly.

Fig -2: ATM after attack [3]

The Malware attacks are carried out through one or more of the four vulnerable components of an ATM.

2.1 ATM computer:

A malware or any malicious coding could be used to attack and take control of the computer system and make a new set of commands to dispense cash. A criminal is able to infect the ATM with malware and can access these devices or directly connect their own equipment to the dispenser or card reader. By design, an ordinary ATM user interacts with only one application which runs in kiosk mode. By exiting kiosk mode, an attacker could bypass these restrictions and run commands in the ATM operating system.

2.2 Card reader:

Skimmer devices could be installed for stealing the card information and then use to withdraw money from other account holders.

2.3 Cash dispenser:

The cash dispenser is located within the safe, which is physically well protected. But the connection of the cash dispenser to the ATM computer is located outside of the safe, and therefore easy to access. In some cases, criminals have drilled holes in the front panel of an ATM in order to access the dispenser cable. With such access, criminals can then directly connect the dispenser to their own device, which is programmed to send cash dispensing commands. This device is most often a simple single-board computer running modified versions of ATM diagnostic utilities. Diagnostic utilities usually run checks to verify that access is legitimate, but attackers know how to disable these checks and any other security mechanisms. These techniques are combined in what are known as Black Box attacks.

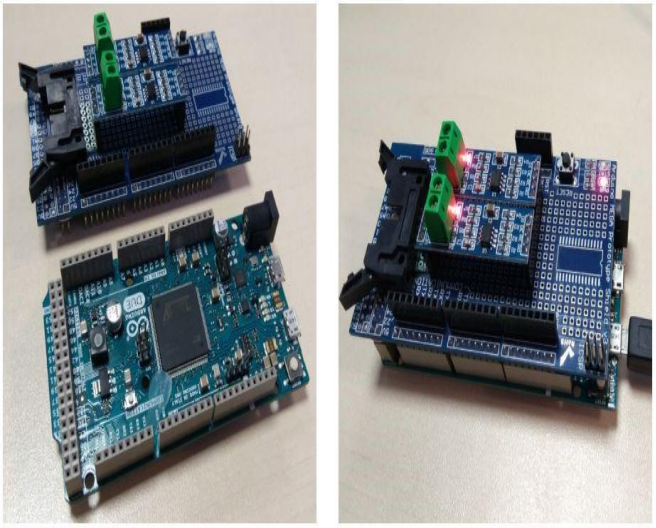

Fig -2: Black box [2].

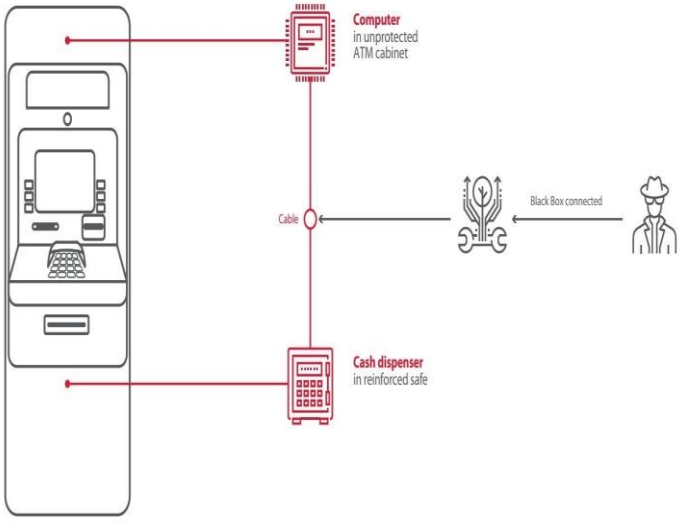

Fig -3: black box attack [2].

2.4 Network equipments:

For network-level attacks, the main requirement is access to the network to which the ATM is connected. An attacker physically opens the ATM, unplug the Ethernet cable, and connect a malicious device to the modem (or replace the modem with such a device) [2]. Then it is possible to connect to the device and attack available network services or attempt man-in-the-middle attacks. A criminal with access to the ATM network can target available network services, intercept and spoof traffic, and attack network equipment. An attacker can exploit vulnerabilities in available network services, and thereby execute arbitrary commands for disabling security mechanisms and controlling output of banknotes from the dispenser [4-5].

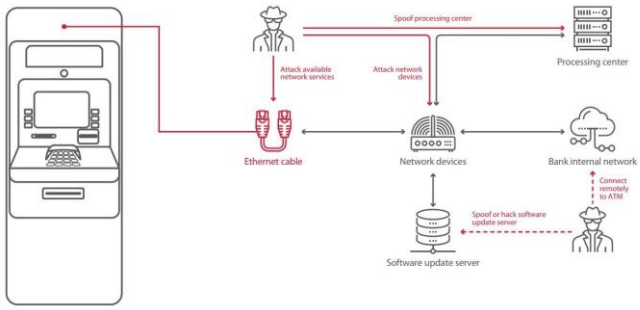

Fig -4: ATM Network attacks [2].

3. CASE STUDY

An ATM in a remote kiosk, was attacked, cash dispenser was found in open condition and the money was found missing. It was suspected to be a case of ATM hacking/jackpotting. For investigation of the case, two hard disk drives attached to the ATM computer system were received in the Forensic Laboratory. The bit stream images of the hard disks were obtained and forensically analysed. It was required to know, how the attack happened, what was the intruder software and through which IP address attack

was carried out. On analysis of first hard disk, it was found that few files were encrypted with the time stamp same as that of the date/time of ATM attack which suggested an external interruption. The encryption prevented the normal course of working of the ATM and thus became susceptible to attack. A trace of file "setup.msi" was found and matched with the suspected data/time of attack. As per the Meta data of the setup/ installation file, the last saved name was "DavidHacker" and this could be inferred as the malware used for attack.

The second hard disk contained frames of image files captured through the camera in front of the ATM. Image files of the relevant time period was studied and found that a male person was trying to operate the ATM during the suspected time of attack. The image files captured contained the date/time stamp along with the IP address of the system written on it. As the person was trying to operate the ATM and infecting the system with malicious software, the IP address displayed on screen was found to be changed to a new IP address. The change in IP address clearly suggests the new IP address through which the attack was carried out. Based on the image captured of the suspect in ATM, a male suspect was identified. The images captured in the camera and that of the actual image of suspect were compared and found to have matched.

The hard disk analysis is a dead analysis, where all the details of processes running on the computer and data stored in the volatile memory is not available inclusively. Trace analysis of the files is required which needs to be strategized on the type of the files and data/time stamp required. This method brought fruitful results where, the suspect who had carried out the ATM attack was identified and the software tools & modus operandi was successfully identified.

4. CONCLUSIONS

The cases of ATM hacking/jackpotting are growing in popularity, all over the world with losses running in to millions of dollars. Identifying and uncovering vulnerabilities related to network security, improper configuration, and poor protection of peripherals is the need of the hour. As the difficulty of exploitation rises, the likelihood of crime decreases. To reduce the risk of attack, the first step is to physically secure the ATM cabinet and surroundings. Exploiting most of the vulnerabilities would be impossible without access to the on-board computer and peripheral ports. Regular security analysis of ATMs is important for timely detection and remediation of vulnerabilities. Security analysis may also include reverse engineering of ATM software, such as Application Control, XFS-related software, and network equipment firmware. Such testing offers uniquely powerful results, due to identification of zero-day vulnerabilities and subsequent measures to protect against novel attack vectors.

ACKNOWLEDGEMENT

We are thankful to the Director, CFSL, Kolkata for his constant support and guidance.

REFERENCES

[1] Cashing in on ATM Malware- A comprehensive look at various attack types; David Sancho, Nurmaan Huq & Massimilianio Michenzi.

[2] ATM hacking report: Scenarios from 2018 ATM hacks, Alex Rolfe, Nov 19, 2018 Daily News, https://www.paymentscardsandmobile.com/atm-hacking-report.

[3] Three arrested for blowing up ATMs in Germany and Hungary, 11 December 2019, News Article, https://www.europol.europa.eu/ newsroom/news/three-arrested-for-blowing-atms-in-germany-and-hungary.

[4] ATM logic attacks: scenarios, 2018, November 14, 2018, Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018.

[5] Criminals Use New Software to "Jackpot" ATM Machines, Laura Bednar,https://www.securedata.com/blog/criminals-use-new-software-to-jackpot-atm-machines.

AUTHORS

M.Maheswari, Scientist-B(Physics), CFSL, Kolkata.

Shashikant Thube, Ex-Forensic Professional, CFSL, Kolkata.

K. B. Jena, Deputy Director & Head of Div. (Forensic Electronics), CFSL, Kolkata.

Dr. P. Paul Ramesh, Assistant Director & Head of Div.(Physics), CFSL, Kolkata.