Secure Transaction in ATM using IOT Bank Server

Harshitha
Department of Computer Science And Engineering
GSSSIETW, Mysuru

Usha Rani J
Assistant Professor, Department of Computer Science And Engineering GSSSIETW, Mysuru

Jayasheela C K
Department of Computer Science And Engineering
GSSSIETW, Mysuru

Meghana M M
Department of Computer Science And Engineering
GSSSIETW, Mysuru

Ranjitha C M
Department of Computer Science And Engineering GSSSIETW, Mysuru

***Abstract* — In 2017 a major holding banking company in Asia conducted an assessment on operational risk associated with ATM's and Point of Sale (POS) Card processors in the Asia-Pacific region. The study showed that 70 % of their incidents occurred in India and Thailand, which subsequently drove them to new and innovative methods to counter the criminals and mitigate the threat. The primary tactic for this theft is "skimming," a process in which your card's magnetic strip is scanned and recorded on a hard disk drive (HDD) to be later paired with your PIN code and used to access your account. Today's thieves are getting more technical and tactical in their efforts to steal your property and, in some cases, personal identity. In this proposal we are designing a unique IOT server to manage the transaction details of the consumer with android mobile. Instead of POS card process we are planning to use the user's mobile as a transaction device, and the ATM machine is only the Money receiving Unit.**

Keywords— IOT server, mobile application, Bank server,ATM server.

I. INTRODUCTION

Forty-nine years ago, if you needed cash you had to head to your bank and request it from the clerk at the counter. But on the 27th of June 1967, all that changed. On that day Londoners had their first opportunity to withdraw funds from their accounts via a new specialized cash machine, which later became known as an automated teller machine, or ATM for short. Since then, this technology has taken over the world, placing close to three million machines around the globe and still adding on average 280 new machines every day. Apart from the convenience ATMs have brought to regular users over the years, they have also attracted the attention of criminals. With space for thousands of bank notes in each machine, the potential gain is so high that some criminals are still trying, via brute force, to liberate the contents (and by that we really mean using brute force) ripping machines from walls or stealing them whole. Others opt for more sophisticated methods, such as building bogus parts for the machine that are very hard to spot, a.k.a. skimmers. These include fake panels, displays, PIN pads, card acceptance slots, hidden cameras and of course their combinations. If criminals succeed in their attempts, they can use the obtained data to impersonate their victims, empty the account or sell the information to other malicious actors online. However, the latter option is not very lucrative anymore as prices for payment card data have slumped from hundreds of dollars per (corporate) card in 2010 to just a few dollars at present. Last but not least, there are also attackers that focus mainly on the software flaws in ATMs. Unfortunately, cracking ATM security is sometimes less difficult than it should be. A large chunk of ATMs still run outdated or unpatched software such as Windows XP or Windows XP Embedded (in 2014 this still represented 95% of all machines worldwide), both of which are beyond the end of their lives.As reported in a series of blogs by security researcher Brian Krebs, cybercriminals are trying various tricks to make the machine spit out cash. One of them is to connect via its USB ports hidden behind the outer shell and then installing malware that will release the cash. Some ATMs still automatically run anything on an inserted USB device and can easily get infected. Last year, skimmers also came up with a new type of assault dubbed "black box". After disconnecting the ATM's cash dispenser from the core of the machine, they connect their own small computer, issuing fraudulent commands that release cash. Another technique observed in the wild was misuse of the machine's internet or phone cable connection for man-in-the-middle attacks, intercepting customer information on its way online.

So what does this mean for you as a regular ATM user? Customers are mostly targeted by hardware techniques and thus it is better to be aware of and know how to spot them. To make it easier, we've complied some of the advice offered by banks and law enforcement agencies for you.

II. IMPLEMENTATIONS

Security Management Platform:Enterprise application bus (Internal Event Bus) that enables the cooperation among

different modules. Another application bus (External Event Bus) is used to connect the national level SMP to the European level SMP and to local security systems such as LGSOCs and other security prototypes.

Command and Control subsystem:This subsystem provides Alarm Correlation, Security Monitoring and Decision Support for Incident/Crisis Management. It includes a Data Collector for gathering security events from Local Security Systems and ATC systems, correlating them using a Correlation Engine and displaying

the resulting alarms to the operator with the Monitoring facility.

Cyber Security Intelligence Platform:

The Cyber Security Intelligence Platform (CSIP) is based on an open source intelligence service provided in cloud by Finmeccanica. The intelligence module is connected to the Command and Control module by API connection . CSIP provides GAMMA operators the possibility to obtain relevant information about possible (cyber) attacks on ATM systems, crawling the internet though open sources such as social networks, in order to determine the sentiment and/or threats related to a particular target. They also allow to identify the motivation, the characteristics and the identities of the attackers.

Attack Effect Prediction Module:

As was stated before, the SMP serves as a central collector and analyzer of the information generated by diverse set of security controls and event detectors. In this case the joint and sequential analysis of the received information may serve a crucial task, as the Data Fusion enabled by the SMP may reduce the number of false alerts and enable temporal analysis of the actions of the adversary.

The Attack Effect Prediction (AEP) Module is a decision support SMP sub-system that provides a joint assessment of the information received from different sensors (event detectors) represented at the system.

III. SYSTEM DESIGN

In this Proposal we will use smart phone as a POS card, by using the app user can communicate with the IOT bank server to verify him as genuine customer, then server open the ATM machine to withdraw the money from machine. User need to add or uses the machine to receive the money how much he wants, and need to not clear once after the money he received. And transaction details will be stored in cloud server In this case user need not worry about Skimming and any other data loss.

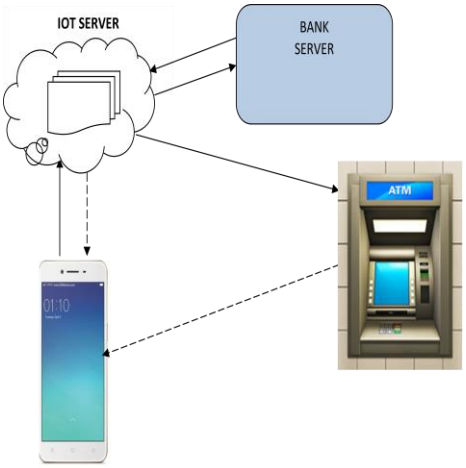

Fig: System Architecture

Account:

a single account in a bank against which transactions can be applied. Accounts may be of various types with at least checking and savings. A customer can hold more than one account.

ATM:

A station that allows customers to enter their own transactions using cash cards as identification. The ATM interacts with the customer to gather transaction information, sends the transaction information to the central computer for validation and process-ing, and dispenses cash to the customer. We assume that an ATM need not operate independently of the network.

Bank:

a financial institution that holds accounts for customers and that issues cash cards authorizing access to accounts over the ATM network.

Bank computer:

the computer owned by a bank that interfaces with the ATM network and the bank's own cashier stations. A bank may actually have its own internal network of computers to process accounts, but we are only concerned with the one that interacts with the network.

Mobile to Cash:

A mobile app given to a bank customer that authorizes access to accounts using an ATM machine. Each app contains a bank code and a secret number, coded in accordance with national standards on app ids and cash cards. The bank code uniquely identities the bank within the consortium. The App ID determines the accounts that the cash can access. A app does not necessarily access all of a customer's accounts. Each cash app is owned by a single customer, but multiple copies of it may exist, so the possibility of simultaneous use of the same app from dierent machines must be considered.

Customer:

the holder of one or more accounts in a bank. A customer can consist of one or more persons or corporations the correspondence is not relevant to this problem. The same person holding an account at a dierent bank is considered a dierent customer.

Transaction:

a single integral request for operations on the accounts of a single customer. We only specified that ATMs must dispense cash, but we should not preclude the possibility of printing checks or accepting cash or checks. We may also want to provide the exhibility to operate on accounts of different customers, although it is not required yet. The different operations must balance properly.

IV. MOTIVATION

Skimming occurs when a tiny portable device is attached to a card scanner on an ATM machine, at a gas pump, at a restaurant or anywhere else. The device captures your card's information as the magnetic strip passes through the scanner and provides criminals everything they need to steal your identity and funds from your account. There's also the threat of cameras recording your keypad entries or high-tech devices that record your PIN as you enter it. When you're using an ATM or any card reader, take these precautions:

- Take a close look at the card reading slot to determine if there are seams or gaps in the surrounding plastic or if anything else shows an indication of tampering
- Pull on the card reader; if it moves, don't use it.
- Look at other card readers near you to determine if they look the same as the one you're using.
- Use ATMs that are inside a store because it's more difficult to install a skimmer with employees nearby.
- Choose the "Credit" option during purchases to avoid entering your PIN.
- Shield the keyboard when entering your PIN and be aware of your surroundings when using an ATM or any other card reader.

V. CONCLUSION

Since then, this technology has taken over the world, placing close to three million machines around the globe and still adding on average 280 new machines every day. Apart from the convenience ATMs have brought to regular users over the years, they have also attracted the attention of criminals. With space for thousands of bank notes in each machine, the potential gain is so high that some criminals are still trying, via brute force, to liberate the contents (and by that we really mean using brute force) ripping machines from walls or stealing them whole. Others opt for more sophisticated methods, such as building bogus parts for the machine that are very hard to spot, a.k.a. skimmers. These include fake panels, displays, PIN pads, card acceptance slots, hidden cameras and of course their combinations. If criminals succeed in their attempts, they can use the obtained data to impersonate their victims, empty the account or sell the information to other malicious actors online.

REFERENCES

[1] GAMMA Consortium – Description of Work – Part B – September 2013
[2] GAMMA Consortium, GAMMA CONOPS, The Ultimate ATM Security Framework, Newsletter, Issue No 1, pp. 2-3, 2015.
[3] GAMMA Consortium D6.3 Prototypes design and development, 1st release – March 2016
[4] National Security, When Time is of the Essence, Strijland W, 42 Solutions, ATCA Conference Proceedings, Winter 2014: www.atca.org/2014-Conference-Proceedings
[5] Apache Kafka: www.kafka.apache.org.
[6] Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management, Shahbazian, E., Rogova, G., Valin, P, ISBN print 978-1-58603-536-5.
[7] Models for nuclear smuggling interdiction. IIE Transactions, Morton, D.P., Feng, P., J., S.K. 39(1), 3–14 (2007).
[8] Sonar tracking of multiple targets using joint probabilistic data association, T. Fortmann, Y. Bar-Shalom, and M. Scheffe, IEEE Journal of Oceanic Engineering, vol. 8, no. 3, pp. 173–183, July 1983