International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 11, Number 6 (2018), pp. 845-852
© International Research Publication House
http://www.irphouse.com

Mitigation of Cyber Terrorism at ATMs, and Using DNA, Fingerprint, Mobile Banking App to withdraw cash (Connected with IoT)

Nachaat AbdElatif Mohamed[1]

School of Computer Sciences. Universiti Sains Malaysia, Penang, Malaysia

Aman Jantan[2]**, Abiodun Esther Omolara**[3]

School of Computer Sciences. Universiti Sains Malaysia, Penang, Malaysia.

Abstract

Hackers have always targeted automated teller Machines (ATM). Securing ATMs is a concern for most banks in the world, some of them use the keyboard and other using fingerprint, or Wi-Fi, or RFID, Attracting customers will be through new services, but every new service brings with it a new danger, threat, risk, and new techniques from the cyber terrorism strikers to attack it. In this project we will present how to withdraw cash from ATMs through using customer fingerprint from his mobile, and DNA through his watch, we will improve the security of protecting customers, and banks against man-in-the-middle (MITM), eavesdropping, Factum attacks, and reduce the time from 30 seconds to 4 seconds, it is a novel contribution. This paper using ATT&CK as a countermeasure. Our project can implement as a part of IoT, and the separate project is taking into consideration improved security.

Index Terms: ATT&CK, DNA, Eavesdropping, MITM, IoT.

I. INTRODUCTION

Carbanak is an APT-style expedition targeting (but not limited to) financial organizations both public and private, the story of Carbanak began when a bank in Ukraine asked for an investigation In the theft of money from the ATMs, when the team of investigators began to develop a scenario that there are malicious programs, they expected will find a malicious Apps, but after checking the hard drive of ATMs, they did not find anything except, only they found VPN configuration with netmask 172.0.0.0, in that time they consider malware attack, but unfortunately after month's they informed the Russian bank send the money to the persons in the Republic of China, [6]. Carbanak discovered in 2014, [7]. This research project we will produce a new idea, to withdraw cash, and improve ATMs security transactions. Our project will present two major contributions:

- We show, how to withdraw cash through person DNA (using his smart watch), or withdraw cash through person fingerprint (using customer mobile).
- Secondly, we pictorially demonstrate how to enhance the security of the bank, customer, ATM Machine, and we will describe how is no need to use a one-time password pin when to make this operation, (implement our project, DNA, or Finger Print).

- **Note**: I am trying to implement a new concept

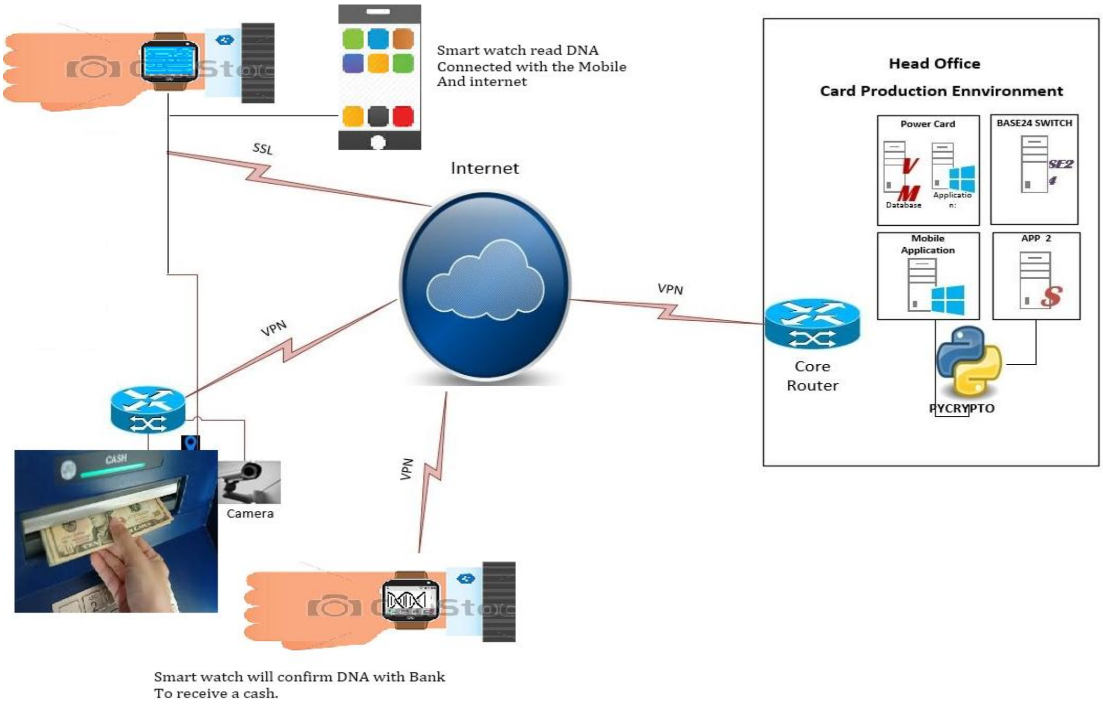

Fig 1 Our Project design (DNA Scenario).

II. TERMS AND BACKGROUND

Jackpotting: Is a sophisticated crime, in this way a hacker can install a malicious application on ATMs machine and force is to get massive amounts. By Jackpotting Exploit Hacker can "analyse the internal structure of their code", [5].

man-in-the-middle attack (MITM) this kind of attack is, attacker keeps himself between 2 points, client with the server, or a client with the client, etc., and give them feeling they are discussing with each other Without any interference from anyone over privet connection, but in fact, the hacker manage, monitor, and control everything, [3]. The hacker can see the content traffic between 2 points (usernames, Passwords), [4].

Shoulder surfing Shoulder surfing is techniques using directly to stealing a password or pieces of information, and it is a beneficial way to get information over shoulders especially in crowded places, imagine you are front of ATM, try to withdraw cash, and another person behind you in the queue, scanning your pin ATM code over your shoulders.

IoT Internet of Things, is the network of real devices, vehicles, mobile, tablets, laptop, home devices and other parts installed with many thingis , sensors, software, Recent research predicted that by the year 2020, about fifty (50) billions of such devices are expected to be deployed [2].

III. STATE-OF-THE-ART

We provide a summary of existing literature that is closely related to this research.

Kumar et al [8] we are used sixth sense technology to allow us access by gestural interface to do the all transaction of cash operation.

Kaczmarek et al [9] When the people using keyboards to enter a pin code, they automatically leave thermal residues at that keyboards, the attackers can read this information by using some terminators after short time, this kind of attack called (Factum attack) gives very accurate results.

Alhassan et al [10]. The strikers can tack sensitive information through Salami fraud or Salami attack, this kind of attack occurs when the hacker acquired a piece of information from deferent sources, and use it to attack organizations, the remedy this kind of attack we can achieve it by ethical hacking.

Nachaat et al [1] we will use mobile App, finger print (from ATM), and PY crypto to withdraw cash from ATMs and improve security level for customer and bank against eavesdropping attack.

IV. PROJECT PROPOSAL (SOLUTION)

The motive of our project withdraw cash from ATMs through mobile banking Apps by using customer DNA, or fingerprint (we will use customer fingerprint from his mobile, not from ATMs), to decrease the customer time, and improve the security against eavesdropping, the man in the middle, and Scamming Attacks. We will try to cover the most important point in this project, the first Scenario, through using customer DNA (it's highly privacy protection), before present this scenario we recommend Samsung, apple, and other companies to develop a new smartwatch can read DNA of humans. First of All, the bank must request from all customers to update those data, to allow the bank registering customer DNA long number in Database. Second let's jump if the customer needs to withdraw a cash from ATMs through his DNA, and using his mobile, through the smart watch or mobile he will use mobile bank app and request to withdraw some money for example 300 $, in same request mobile, or smart watch will send the customer location, after bank receives the request, (based in that request bank will knows, all customer details, Including Customer DNA)bank application will fetch automatically list of ATMs Machines which located in same customer area, Based on people front of each machine and nearest machine from the customer, third, the bank will send message to customer, ask him to go this machine (best solution), and ask him when you be front of ATM confirm this message from your smart watch, forth, customer now front of ATM, he confirmed the bank message, the smart watch will read the customer DNA and send it to the bank to compare with bank database, if approved, directly the 300 $ will comes out without using any card or pin.

Second Scenario, Using customer fingerprint from mobile it is a new technique, and great service for the banks can use it to bring more customers, to participate based on quality, security, smooth, and speed. Before everything, Bank must request from all customers to update those data, to allow the bank registering customer fingerprints in the bank database, and convert this fingerprint to the encrypted number by PY crypto, then let's go for our novel scenario. The customer will start to request withdraw money through Mobile Banking application, This request which happened by customer will take customer location to the bank in the same message, Second after the Bank receive the customer request, bank application will fetch automatically list of ATMs Machines which located in same customer area, Based on people in front of each machine and nearest machine from the customer, third, The customer receive the reply message from the bank at his request guide him to go to the beast solution near from him Chosen by the bank, Fourthly, The customer Will follow Bank instructions in the message Which includes, reach to machine which Identified by bank, and Confirm this message when you are front of the ATM machine, Finally, When the customer front of ATM machine, and confirm the message, the application well present fingerprint field on the mobile screen, Ask the customer put your fingerprint please, (Just the customer punish his fingerprint On his mobile, the cash, which identified on the first request by customer, (will come outside the machine directly).

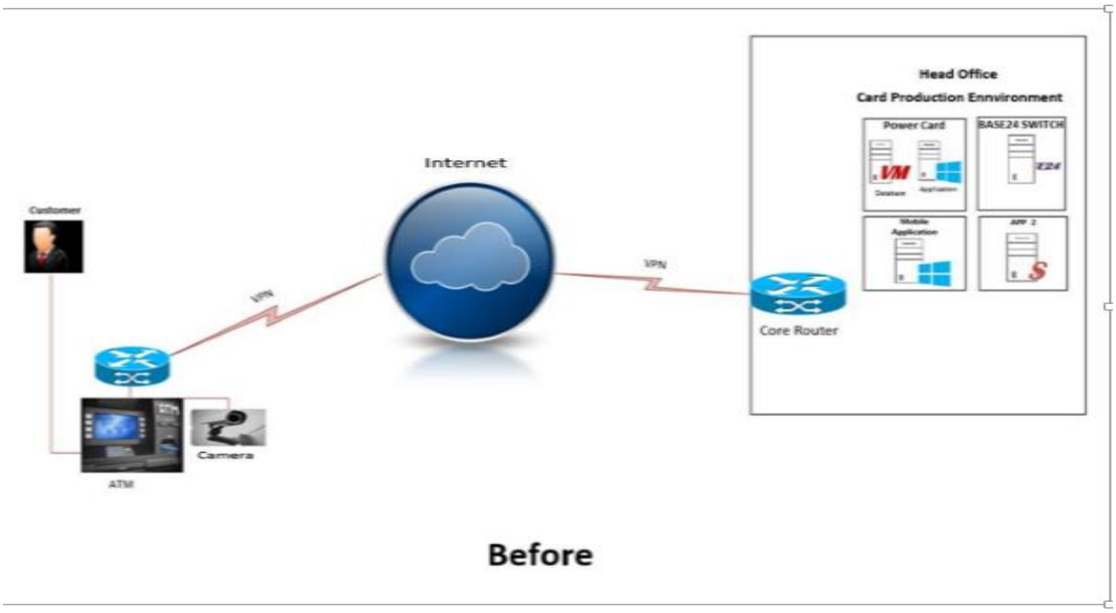

Fig 2 ATM before using our design (DNA, or Fingerprint Scenarios).

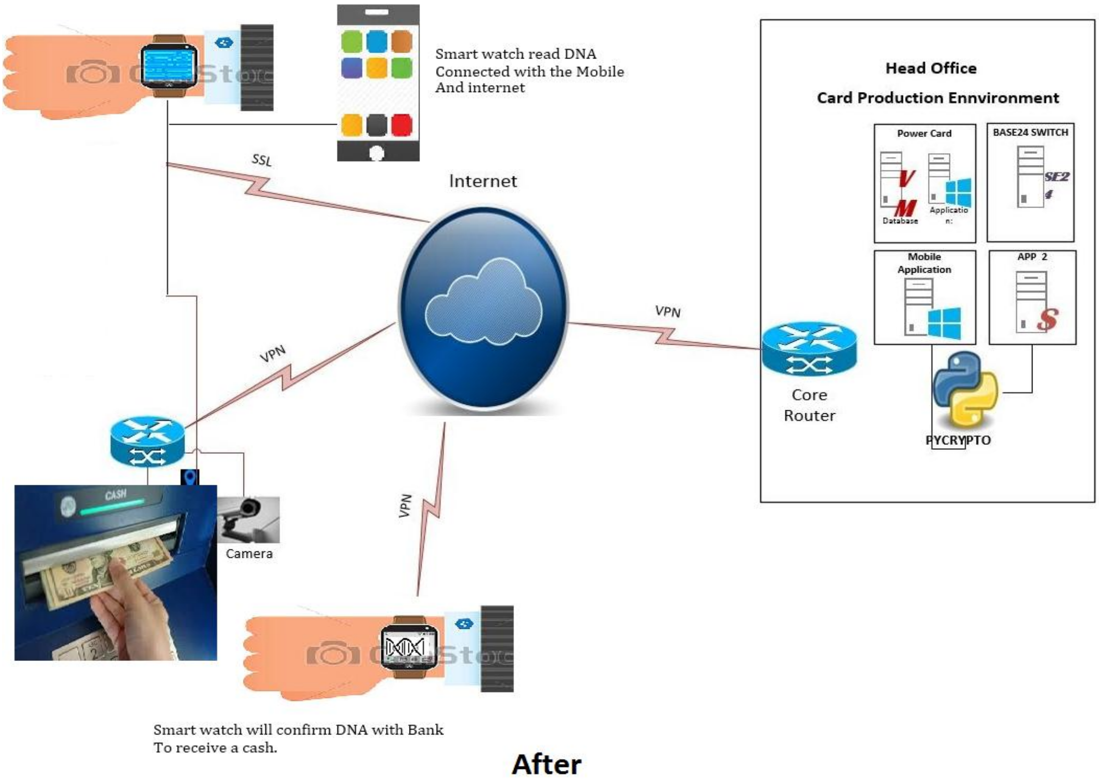

Fig 3 ATM before using our design (DNA Scenario).

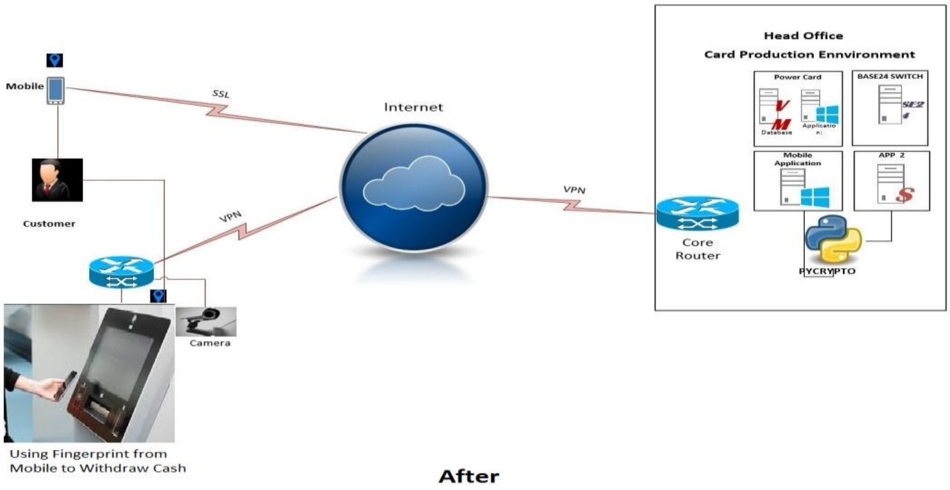

Fig 4 ATM after using our design (Fingerprint Scenario).

V. EXPECTED RESULTS

This research aims at presenting a new method to withdraw cash from ATM through customer DNA, and fingerprint (DNA will read automatically through smart watch), (the customer will hit fingerprint from his mobile). After applying for this project. This research is highly profitable for industries especially if implemented in specific country's (developing, and developed countries). Reduce customer time from 30 seconds to 4 seconds, make withdraw cash easy, enhance the security of banks and ATMs, and improve the security customer privacy. Finally, we can customize the project as appropriate for each country, avoid any attacks like (Scamming, Factum, Shoulder Serving, Eavesdropping, and MITM), and the system can be integrated easily with the Internet of things (IoT).

VI. CHALLENGES

In our project, we faced difficultyas the most banks declined to cooperate with us due to, we need interaction with some banks to study the real situation, cost, Enactment to obtain customer DNA, fingerprint, and devices.

VII. RESEARCH GOAL

The most important two objects of this project are, keeping the customer time while taking outperformance, and an improvement in the security level which currently is not recommended in traditional ATM setting. Usually, a customer wants about thirty (30) seconds or more to get his money from ATMs, but the approach intended in this article will let the same event for a shorter period of (4) seconds. On the other hand, we increased the protection, and security, in defending private communication between customers, mobile app, and ATMs against Scamming, eavesdropping, Factum, and MITM attacks. After applying our project, no need for OTP, we will compare The real DNA very long encrypted number with the same which stored in bank database, or using the second scenario, customer will use his fingerprint from his mobile, the person can withdraw his money in 4 seconds. This feature will add value to the bank's services; the bank can sell it to attract the customer.

VIII. CRITICAL SCENARIO

- Use fingerprint from ATMs to withdraw cash.
- Use fingerprint from Mobile to withdraw cash.
- Using DNA to withdraw cash.
- Use D.QR-code to withdraw cash.
- Use Barcode to withdraw cash.

IX. CONCLUSION

In this paper, we have presented how to use customer DNA, and fingerprint from his mobile, or his smart watch to withdraw the cash, in addition, glamorized a critical scenario, D.QR-code, Barcode, finger eye, and fingerprint to withdraw cash. We described how our contribution can reduce the time, effort, and improve the security, secure banks, and customers against Scamming, eavesdropping, Factum, and MITM Attacks. We encourage Samsung, Apple, and other companies to design smart watch can read person DNA automatically, this will help a scientist, and professional persons in many projects to serve humanity, improve the security projects, and save the privacy of people.

ACKNOWLEDGMENT

This research was partially supported by the Fundamental Research Grant Scheme (FRGS) for ‘‘Content-Based Analysis Framework for Better Email Forensic and Cyber Investigation’’ [203/PKOMP/6711426], Security and Forensic Research Group (SFRG) Lab, School of Computer Sciences, Universiti Sains Malaysia.

REFERENCE

[1] Mohamed, Nachaat AbdElatif, Aman Jantan, and Abiodun Esther Omolara. "Using Fingerprint, Pycrypto, and Mobile Banking App, to withdraw cash from ATMs in Developing Countries.(A Confrontation to Eavesdropping Attack based on One-time Password (OTP))." (2018).

[2] Sheth, Amit, Biplav Srivastava, and Florian Michahelles. "IoT-Enhanced Human Experience." IEEE Internet Computing 1 (2018): 4-7.

[3] Tanmay Patange (November 10, 2013). "How to defend yourself against MITM or Man-in-the-middle attack".

[4] "Network Forensic Analysis of SSL MITM Attacks". NETRESEC Network Security Blog. Retrieved March 27, 2011.

[5] Johnson, Michael, and Perdita Stevens. "Confidentiality in the Process of (Model-Driven) Software Development." (2018).

[6] Kaspersky Labs' Global Research & Analysis Team (GReAT) (February 16, 2015).

[7] Kaspersky. Retrieved 12 June 2017.

[8] Kumar, S. Pradeep, and N. Shanmugasundaram. "Pin number theft recognition and cash transaction using sixth sense technology in ATM/CDM." International Journal of Engineering & Technology 7.2.31 (2018): 178-180.

[9] Kaczmarek, Tyler, Ercan Ozturk, and Gene Tsudik. "Thermanator: Thermal Residue-Based Post Factum Attacks On Keyboard Password Entry." arXiv preprint arXiv:1806.10189 (2018).

[10] Alhassan, Nazifi Sani, et al. "Salami Attacks and their Mitigation-An Overview."

[11] Hajare, Uday, et al. "Efficient Cash Withdrawal from ATM machine using Mobile Banking." (2018).

[12] Mahapatra, Durga Madhab, and Soumendra Kumar Patra. "Electronic Payment Adoption In India: Development And Policy Issues." Aweshkar Research Journal 24.1 (2018).

[13] Ngalo, Tamsanqa, et al. "Threat Analysis of Software Agents in Online Banking and Payments."

[14] SENANAYAKE, Tharindu, and Suchinthi FERNANDO. "Information Security Education: Watching your steps in cyberspace." The Online Journal of Science and Technology-April 8.2 (2018).

[15] Botchwey, Gabriel. "E-Governance and Cybersecurity: User Perceptions of Data Integrity and Protection in Ghana."