ATM Security: A case study of Emerging Threats

Ella Nsonta Kasanda
School of Engineering
University of Zambia
Lusaka, Zambia
e-mail: ellah.kasanda@yahoo.co.uk

Jackson Phiri
School of Computer Science
University of Zambia
Lusaka, Zambia
Jackson.phiri@gmail.com

Abstract—Automated Teller Machines(ATM) have gained popularity in the banking sector due to the number of advantages they offer to ATM users. ATM users are able to withdraw cash, make cash deposits, make balance enquires and pay bills without having to go into the branch and experience the undesirable long ques. ATMs have however brought with them cyber-crime in which ATM users and banks lose huge amounts of money. ATM crime has continued to grow and spread globally despite the regional variation of the frequency of the crime. Commercial banks and IT security professionals around the world have concentrated on fighting traditional ATM crimes like ATM card Skimming. However, new ATM crimes like Jackpotting and Shimming attacks have emerged. These logical attacks have continued to grow in the recent years. In this case study we used a risk management framework to determine traditional and emerging ATM crimes, and made recommendations on measures ATM owners can put in place to mitigate both the traditional threats and the emerging threats. ATM software whitelisting was recommended to help fight logical and new crimes like Jackpotting which can't be mitigated using traditional ATM security measures like Payment Card Industry Data Security Standard (PCI DSS).

Keywords-component; Automated Teller Machine, ATM Fraud, Jackpotting, Shimming, Skimming

I. INTRODUCTION

Automated Teller Machine (ATM) fraud has become a global issue that faces not only customers, but also bank operators and has been on the rise in the recent years [1]. Fraud techniques used by cyber-criminals have become more advanced and managing the risk associated with ATM fraud as well as diminishing its impact is an important issue that face financial institutions around the globe. Cyber-criminals are moving away from the traditional ATM card skimming attacks to new attacks such as ATM Jackpotting and ATM card Shimming. With the coming of the new ATM attacks, ATM owners have a task of ensuring that they are cyber ready for these new threats.

In 2013, several commercial banks in Zambia were robbed of more than US$4 million, through a sophisticated cyber-crime syndicate by foreigners who connived with Zambians [2]. The cyber-criminals used ATM card skimming techniques to copy customer's data from magnetic stripe ATM cards. They used the data to reproduce the ATM cards that they used to steal money from the customer's accounts. Commercial banks introduced the Europay, Mastercard, Visa(EMV) chip and pin ATM card to help mitigate the ATM card skimming Attacks in Zambia. Bank of Zambia mandated all commercial banks to migrate to EMV chip and pin card by 31st December 2015. All this is in an effort to help fight ATM fraud and to reduce the financial loss being faced by both the commercial banks and the ATM customers.

However, ATM cyber-criminals have moved a step forward and new ATM threats have been introduced. In January 2018, a total sum of US$1 million was stolen from various ATMs in the United States of America(USA) through Jackpotting Attacks [3]. The fact that this crime happened in the USA doesn't mean other countries around the globe are not at risk as cyber-criminals in the past have been seen to attack and move to another location. This therefore is an emerging crime that all ATM operators globally should get prepared for.

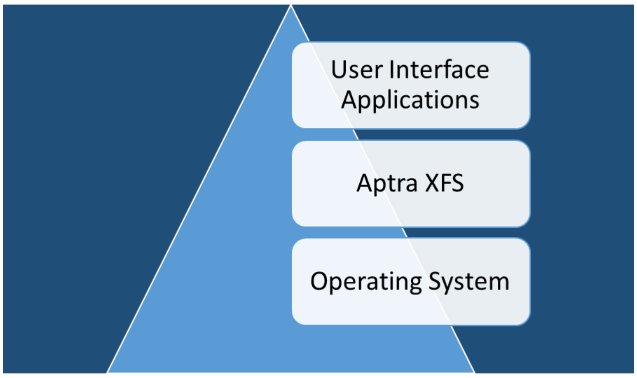
In order for Zambia to be cyber-ready for these new ATM crimes and the already existing ones, this study will use a risk management framework to determine the risks that are faced by ATMs in Zambia and around the globe. We will identify the asset that should be protected, and then identify the ATM threats and vulnerabilities after which we will make recommendations on countermeasures that will help mitigate ATM risks and commercial banks can adopt them.

Part II of this paper explains the logical design for the ATM software, part III reviews ATM threats, part IV outlines the case study conducted on ATM risk management, part V presents the discussion which includes the recommendations, part VI discusses related works, part VII presents the conclusion and part VIII makes suggestions for future work.

II. LOGICAL ATM SOFTWARE DESIGN

Fig. 1 shows the logical design of an ATM's software. The PC of an ATM is first installed with an operating system like windows XP and windows 7. Aptra XFS is then installed on the PC to enable the PC communicate with the different physical devices of the ATM like card reader, cash dispenser, receipt printer, journal printer, encrypting pin pad and cash depository for the ATM models that are capable of accepting cash deposits. An application that customers will interact with as they are using the ATM is then installed on top of Aptra XFS. Different ATM software vendors call this application different names like Aptra NDC, Aptra YDC and BWAC. This is the application that also speaks to the ATM switch.

FIGURE 1. ATM SOFTWARE LOGICAL DESIGN



III. ATM THREATS

ATM threats/attacks can be divided into physical and logical attacks. Physical attacks involve attacking the ATM physically like exploding the ATM safe to have access to the ATM safe money. In physical attacks, cyber-criminals use methods such as solid and gas explosives, as well as uprooting the ATM from the site and then using other methods to gain access to the safe. Other physical attacks involve placing of gargets on the ATM by cyber-criminals that copy ATM card data and reproduce it on another card that can be used to withdraw money from the cardholders account. Logical attacks involve using malware to instruct the ATM to dispense money. This attack can be achieved by either gaining physical access on the ATM in order to install this malware on the ATM's PC Core or the malware can be injected through the network.

A. *ATM Card Skimming Attack*

ATM card skimming attack is a physical threat which has been the number one ATM threat globally in the past. ATM skimming refers to the stealing of the electronic card data, aiding the criminal to counterfeit the card. A skimmer is a device that is installed on a card reader making a customer believe they are inserting their card in a ATM card reader. The skimmer reads the data from a card's magnetic stripe or EMV chip when a client inserts a card into the ATM. Some skimmers have the capability to read data from an EMV card chip at a distance. ATM skimming attacks are however on the decrease due to deployment of anti-skimming solutions, payment card industry data security standard (PCI DSS), EMV technology and contactless ATM functionality. Customers are unable to notice a problem and experience a normal ATM transaction until their account is defrauded. The most common places where skimmers are placed on the ATM are shown in figure 2. Multifactor authentication using biometrics can be used as an added security mechanism against this type of fraud [4]

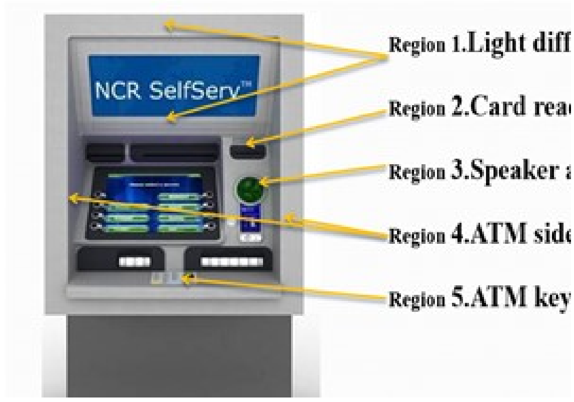
B. *Eavesdropping Skimming Attack*

A new type of skimming attack called Eavesdropping Skimming has emerged and expanded predominantly in the United Kingdom. The attack targets ATM motorized card readers on older model of ATM called personas. However, in the USA this attack occurred on the newer model of ATM called SelfServ [5]. The attacker penetrates the ATM facial to have access to the card Reader of the ATM. A skimmer is then fitted directly onto an electrical node that carries card data on the card reader. On Personas ATMs, the attacker targets the card reader electronic control board by creating a hole behind the ATM card orientation window. In the newer attacks against SelfServ model ATMs, the attacker has changed the method but has maintained the principle. The variance in the way this attack is performed on the two different ATM series shows how sophisticated ATM cyber-criminals are. The ATM SelfServ model targeted is the 6634, which is a Through-The-Wall (TTW) ATM. The attacker makes a hole in the side panel in between the ATM monitor and the card reader. The attacker uses this hole to fit an Eavesdropping Skimmer beneath the card reader connecting directly to the magnetic read head. The hole that was made in the ATM is then concealed by fixing a panel which is the same color as the ATM facial over the entire side panel of the ATM.

C. *ATM Card Shimming Attack*

ATM card shimming attack is a Man-in-the-Middle attack in which the cyber-criminal inserts a device into the ATM card reader that intercepts and records the data flowing between the EMV chip and the ATM card reader [6]. This data could then possibly be reused to clone a magnetic stripe card. EMV chip data and magnetic stripe data have different check values (CVVs) and therefore the data that is captured from the EMV chip card can't be used to clone a magnetic stripe. Card Shimming is neither a vulnerability with a chip card, nor with an ATM. It is therefore not necessary to add protection mechanisms against this form of attack to the ATM. If the proper authorization procedure is followed during an ATM transaction, counterfeit cards can be immediately detected. This attack can only be successful if an issuer neglects to check the CVV when authorizing a transaction. All issuers must therefore make these basic checks to prevent this category of fraud.

FIGURE 2. SKIMMING DEVICE LOCATIONS



D. ATM Card Trapping Attack

ATM Card Trapping steals the physical card itself through a device attached to the ATM. Cyber-criminals place a device directly over or into an ATM's card reader slot. These devices are designed to capture cards after customers' insert them. In a magnetic stripe environment or chip-and-signature environment, the PIN does not need to be compromised and therefore having an ATM is enough to compromise a customer's account. Contactless capability can help against this fraud. For example, National Cash Register one of the world's ATM giants helped launch the world's first tap and pin ATM with ANZ using SelfServ 23 and EMV contactless technology.

E. ATM Cash Trapping Attack

Cash Trapping is where the cyber-criminal uses a device to physically trap the cash that is dispensed and comes to collect it once the customer has left the ATM location [7]. This fraud involves placement of money traps or false presenters in front of the ATM dispenser. When processing a transaction, an ATM dispenses notes into the trap set by cyber-criminals rather than present the money to the customer. The customer assumes the ATM has malfunctioned and leaves. The cyber-criminal then returns, removes the money trap or false presenter, and leaves with cash that was intended for the customer. Cash trapping however mostly succeeds with insider involvement. ATM owners must put measures in place that helps mitigate insider threats.

F. Transaction Reversal Fraud

Transaction Reversal Fraud (TRF) involves the creation of an error that makes it appear as though the cash has not been dispensed [8]. The account is re-credited the amount 'withdrawn' but the criminal pockets the money. It could be a physical grab (similar to cash trapping) or a corruption of the transaction message. This type of attack has occurred in a number of countries including United Kingdom, Ukraine and Canada [8]. The attacker achieves this by creating a fault on the ATM during a cash dispense operation causing the host switch to reverse the transaction. The account will not be debited although the criminal will remove the cash from the ATM. To avoid being caught, attackers use stolen or skimmed cards. The attacker targets TTW ATMs like the NCR 6634 and 6625. The attacker causes an error on the card reader during a cash dispense operation. The correct PIN is entered and cash requested. After the transaction is authorized by the host switch, the ATM counts the cash and positions it behind the cash dispenser shutter awaiting to be dispensed. The card is ejected and the attacker waits for the ATM transaction to time out and attempt to capture the card. At this point the attacker holds the card and prevents it from being captured and then forces the cash dispenser shutter open and removes the stacked cash. The ATM reports a card jam and reverses the transaction.

G. Social Engineering/Phishing Attacks

The Victim is tricked into revealing his/her authentication information (PIN) [9]. It can be physically or through electronic means. e.g., rogue websites are set up by the perpetrators to collect authentication information from un-suspecting customers in the name of necessary updates or changes being carried out by their 'Bankers'. The user ends up divulging his card sensitive data to the rogue site.

H. Operational Fraud

The ATM dispenser is manipulated in this type of fraud. The ATM is configured to dispense big denominations as smaller ones, there-by giving out more money than should be dispensed. This can be achieved by either loading wrong denomination notes in the wrong money cassettes or by making a wrong configuration in the software.

I. Malware Attacks

Malware attacks are usually easier with insider involvement as physical access is necessary to deploy the virus. However, this attack is possible online today. The malware file or device is placed on the ATM; its control device is then triggered to give remote control to the perpetrator through a custom interface which enables capture of card numbers and PINs through the private memory space of transaction-processing applications installed on a compromised ATM. Magnetic stripe cards are very vulnerable to this type of attack. Deployment of effective anti-malware software can help mitigate this class of attacks.

J. Man-in-the-Middle Attack

In 2015 a "Man-in-the-Middle" network attack was detected in Mexico and ATM operators were Alerted [10]. This class of attack occurs when malware is placed within the banks network and compromises the banks network infrastructure. The network traffic is monitored and the malware listens for transaction messages from the ATMs.

When the malware recognizes a cash withdrawal transaction message from a bank card, it intercepts the corresponding host response from the ATM switch and changes the authorized dispense amount to a larger sum than requested and approved by the ATM switch. In order to perform the fraud, an attacker will initiate a withdrawal transaction at any ATM on the compromised bank network. The attacker will use a pre-defined known card number. The transaction will be intercepted and the card number will be recognized by the malware. It will then wait for the host response to the withdrawal request. The malware will intercept the host response message and modify it to a larger amount therefore the ATM will dispense far more money than what is debited from the account. A variation of the attack, is where the malware intercepts the request, and returns an authorization message such that the transaction host is unaware of the request.

K. Ransomware Attacks

A serious malware called "WannaCry" has impacted many organizations worldwide. This type of threat is known as ransomware. It was launched on 12th May 2017 and targeted computers running Windows 7 or earlier in over 150 countries [11]. WannaCry encrypts the files on end-points that are running Microsoft operating system software, rendering them inaccessible. The files are only decrypted upon payment of a sum of money known as ransom. This malware attempts to infect other end-points on the same network. The malware does not specifically target Banking and Retail systems or their functionalities but ATMs like any other Windows based system are also at risk of this attack. There have been unconfirmed media reports that some ATMs in India have experienced this attack. Customers running any Windows OS who have not applied the Microsoft security patch MS17-010 are at risk. In March 2017 ATM manufacturers advised its customers to deploy this patch.

DieboldNixdolf, another ATM giant recommends the use of Terminal Security to disrupt the execution of malware. Terminal security has more than one protection mechanism which includes sandboxing & application behavior whitelisting, extensive buffer overflow protection, memory access protection and DEP protection. For organizations not running Terminal Security Suite, they can use several general guidelines to prevent such attacks:

- Prevention of infection via phishing emails by implementation of technical and organizational measures,
- Segment and secure local area Network(LAN)/ virtual LAN(VLAN) with intrusion detection and prevention mechanisms to avoid infection and distribution of malware via the network,
- All systems should be patched with the latest security patches i.e Microsoft fix MS17-010 (for currently supported Windows OS versions) and emergency fix1 for Windows XP,
- All unused services must be deactivated.

Many organizations worldwide have been impacted by another malware called Petya [12]. This malware encrypts the files on end-points running microsoft operating system (OS) software, rendering them inaccessible. ATMs are at risk of this attack as they run on microsoft operating system. All ATMs running any windows OS which have not been patched with the Microsoft security patch MS17-010 are at risk. If any ATMs are infected/locked with the ransomware, then every other ATM and end-point on the same network must be checked for infection as well. Once the malware infects one end-point on the network it will replicate itself to other vulnerable systems.

L. ATM Jackpotting Attack

The term ATM Jackpotting comes from the term Jackpot. In this type of attack, cyber-criminals get huge sums of money from the ATM at once. Cyber-criminals use two methods to perform this attack:

- Black Box Attack: In 2017 NCR was warned of a number of Black Box attacks in the UK targeted at Through-The-Wall (TTW) NCR SelfServ ATMs [13]. Some of the attacks have been successful. The cyber-criminal needs physical access to the ATM top cabinet which hosts the ATM PC Core and then puts the ATM in supervisor mode. The attacker removes the ATM network cable so that the ATM cannot be monitored by the ATM monitoring desk. The attacker then installs a black box which is a special device programmed to control the ATM cash dispenser. The ATM goes in supervisor mode for the ATM customer but the cash dispenser still remains working. A black box can be controlled wirelessly through a basic smart phone. The attacker uses the smart phone to issue commands for the ATM to dispense cash. The command can be issued continuously until the ATM cash dispenser runs out of money. The attackers then remove the black box device and leaves no trace of it having been installed on the ATM. In previous Black Box attacks against lobby ATMs, the criminal has gained access to the ATM internal infrastructure by opening the top box. TTW ATMs can be attacked by breaking through the fascia in this new attack vector. This is done by drilling holes in the fascia such that the ATM screen can be removed. This removal allows enough access to an internal USB hub where the attacker can connect a Black Box and operate the attack from the street. Other TTW ATMs however have a provision to be opened from the ATM facial and the PC core can be accessed. This attack can take less than ten minutes to completely empty the ATM cash cassettes [14]. Investigators have reported in court documents that one suspect got away with more than $267,000 in just four days. The Secret Service says criminals have already jackpotted more than $3.5 million from ATMs in the USA. This crime is spreading from state to state in the USA and outside the

USA and has affected banks in Massachusetts, Ludlow, Attleboro, Danvers, Boston, London, Germany, Italy and Mexico [14] [15] [16] [17]. This crime is spreading very fast and will soon hit other countries globally if ATM owners do not put in preventive measures. A Supervisory Special Agent with the U.S. Secret Service stated that this crime is likely being carried out by an international criminal group.

- Malware Attack: Malware can be delivered physically by using ATM USB ports or remotely via a compromised banking network. Using a keyboard and command line, the attacker executes the malware. These actions can even be automated so that the malware will work autonomously. The attack can be conducted through the network without physical access to the ATM. The attack is possible when there is no ATM malware protection system and no software whitelisting for the ATM and no authentication is in place for the data exchange between the ATM hardware units and its main application.

IV. Case Study

The aim of this case study is to perform risk management on ATMs. Organizations perform information technology security risk assessments to assess, identify and modify their overall security posture and to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an aggressor's point of view. This process is used to obtain management's buy in to allocate resources and implement the appropriate security solutions. A risk assessment was therefore carried out to help ATM owners assess, identify and modify their overall security posture. The formula used when conducting the risk assessment is:

$$\text{Risk}=\text{Asset}+\text{Threat}+\text{Vulnerability} \quad (1)$$

A vulnerability is a weakness or a gap in a security mechanism that can be exploited by a threat.

A threat is anything that can exploit a vulnerability and cause damage to an asset.

An asset is a component or item of an IT infrastructure that is valuable to an organization. An asset is what we are trying to protect by doing a vulnerability assessment. Assets consist of both tangible and intangible assets that can be assigned value. Tangible assets can be the ATM and intangible assets can be the company's reputation, databases and a company information.

A risk is the potential or likelihood that a threat will exploit a vulnerability causing damage or loss of an asset [18]. A risk is an intersection of a threat, a vulnerability and an asset. The key to understanding the risk to assets is to identify the vulnerabilities and accurately assess the threats.

The study seeks to identify assets which are endangered by threats, that might exploit vulnerabilities, which results in exposure. Exposure is risk, that is mitigated by safeguards. The focus of this study is thus on logical attacks which is an emerging and growing ATM crime and is able to empty an ATM cash dispenser in just minutes.

The risk management process followed in this case study is as follows:

- Identifying assets: The ATM was identified as the asset in this case study. The value of the ATM is not just the value of buying the ATM but also the loss of customer information that bank operators store, the loss of money by both the ATM operators and the ATM customers, and the loss of customer goodwill.
- Identifying Threats: The threats to an ATM were identified and have been discussed in this case study.
- Identifying vulnerabilities: Vulnerabilities in ATM hardware design and in logical design were also identified.

V. Discussion

Based on the threats and vulnerabilities identified in the case study, countermeasures are discussed in this section. ATM owners must deploy solutions to prevent unauthorized deployment of malware on ATMs. Most ATM manufactures have provided solutions and recommendations on how to prevent logical attacks on their ATMs like NCR Solidcore suite for Aptra. The key principles that should be employed to prevent logical attacks are: only authorized code can run, authorized code cannot be tampered with and authorized code can't be hijacked. This means that ATM PC core BIOS must be protected with a password so that no external media can be used to boot the ATM. Hard Disk encryption is an added protection against malware being loaded onto the ATM in an offline mode. PIN data can be protected from malware attacks by using encrypting pin pad firmware prescribed in the PCI framework. Online malware attacks can be mitigated by whitelisting only software allowed to run on the ATM.

TRF depends on the host switch application reversing the transaction based on status information from the card reader alone. To mitigate this risk, the host switch must also check the status of the cash dispenser before a transaction reversal is done. If stacked cash is detected, it must be safely purged before authorizing a transaction reversal. The new S1 cash dispenser has anti-TRF settings known as EPS2 which can be used to report potential fraudulent behavior. The S2 currency dispenser can also be configured such that no money is pre-positioned behind the shutter.

In Shimming attacks EMV chip data is captured and used to clone a magnetic stripe card. Check values for chip cards are different from the ones for magnetic stripe cards. Cloned ATM cards can therefore be immediately detected during transaction authorization. This attack can only be successful if the issuer doesn't check the check value while authorizing a transaction. All issuers must therefore ensure that check values are always checked before authorizing a transaction.

In general, the following should be done by all ATM owners to ensure that their ATMs are secure:

- Follow all the guidelines in the PCI DSS,
- An Intrusion Detection System must be configured to monitor all traffic and alert on any abnormal behavior,
- A firewall should be configured and be kept up to date and should allow only known application traffic inward and outward,
- A patch management program for ATM operating system and applications should be in place to ensure ATM software is well patched,
- Software Whitelisting solution for ATMs should be in place and an anti-virus must be installed and always updated,
- An incident management system must be implemented, and an incident response plan prepared for rapid deployment in case of a compromise. This is to ensure ATM frauds are reported in real time,
- ATM software must be updated regularly,
- All ATM operators should migrate to EMV chip and pin card and should eliminate magnetic stripe fall back. This will mitigate the risk of skimming cards,
- Separate ATM network from the rest of the bank's network by using a firewall and virtual local area networks,
- The ATM PC BIOS must be secured,
- A password policy must be in place to ensure only strong passwords are used on ATMs and each user has their own unique password,
- All communications on the ATM must be encrypted including communication between the PC core and the cash dispenser,
- Unused services and applications must be removed from the ATM to reduce the attack surface,
- Effective anti-malware software must be deployed,
- The PC core operating system must be hardened,
- Implement a role based access control on the ATM environment,
- Penetration testing must be done on the ATM annually,
- Ensure ATM physical security like CCTV and alarms when installing the ATM,
- Install a tool that will ensure the ATM's confidentiality, Integrity and availability.

VI. Related Works

Matthew [19] proposed the incorporating COBIT best practices in PCI DSS for effective compliance and suggested the model needs to be tested in different industry sectors and geographic locations to validate and generalize the model.

Jennia and Tzi-cker [20] discussed the pre-requisite for PCI DSS compliance procedure which is to identify the credit card data flow, specifically, the stages of the card transaction processing and the server nodes that touch credit card data as they travel through the organization. He stated that this pre-requisite poses a challenge to merchants and described a tool that is designed to automate the task of identifying the credit card data flow in commercial payment systems running on virtualized servers hosted in private cloud environments.

Researchers in [21] discussed system user identification and authentication and proposed an embedded fingerprint biometric authentication scheme for Automated Teller Machine (ATM) banking systems.

A multifactor (PIN and Fingerprint) based authentication security arrangement to enhance the security and safety of the ATM and its users was proposed [22]. A three tier design structure was demonstrated in the proposed system. The first tier concentrates on the biometric feature from enrollment to matching, the second tier concentrates on the database and the third tier concentrates on ATM transactions like balance enquiry and cash withdrawals.

Researchers in [23] analyzed all the issues and challenges that the existing ATM infrastructure has and the ones faced by ATM users. It was concluded that ATMs have become very important to society that many people are dependent on it. The use of biometrics for authentication on the ATM was proposed.

ATM communication protocol was analyzed in [24] and a novel framework for ATM systems that allows entities communicate in a secure way without using a lot of storage was proposed. The architecture and operation of Secure framework for ATMs via secret sharing (SFAMSS) was described in detail. The framework was implemented with Java and its components were studied in detailed. The proposed framework ensures confidentiality and non-repudiation and integrity in communication between bank, ATM, and user.

VII. CONCLUSION

We have discussed several risks that the ATM faces and countermeasures that can help in mitigating these risks discussed. ATM owners should ensure that they employ the recommended countermeasures to ensure the ATM environment is secure for the ATM user. ATM owners should ensure to follow ATM best practices like the PCI DSS in totality in order to reap the benefits of the standard.

VIII. FUTURE WORK

The proposed controls should be validated by implementing them on the ATM and then performing a penetration test. This should be done in different geographical regions to ensure the controls work in all regions of the world. A framework to help enhance ATM security will be developed based on the proposed controls.

References

[1] N. K. Gyamfi, M. A. Mohammed, K. Nuamah-Gyambra, F. Katsriku and J.-D. Abdulah, "Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective," *International Journal of Applied Science and Technology,* vol. 6, no. 1, 2016.*)*

[2] K. Namusa, "Zambia: Cyber Crime Costs Banks U.S.$4 Million," Allafrica, 14 June 2013. [Online]. Available: http://allafrica.com/stories/201306141287.html. [Accessed 28 February 2018].

[3] J. Bloomberg, "ATM 'Jackpotting' Attacks Reveal Deeper Problems," 12 02 2018. [Online]. Available: https://www.forbes.com/sites/jasonbloomberg/2018/02/12/atm-jackpotting-attacks-reveal-deeper-problems/#5b1147ee6fc3. [Accessed 10 04 2018].

[4] J. Phiri, J. I. Agbinya and T.-J. Zhao, "Biometrics, Device Metrics and Pseudo Metrics in a Multifactor Authentication with Artificial Intelligence," in *Proceedings of the 6th International Conference on Broadband Communications & Biomedical Applications*, Melbourne, 2011.

[5] Owen Wild, "Eavesdropping Skimming Attacks on SelfServ," 30 June 2017. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/ncr_security_alert_2017_08_eveasdropping_attacks_v2.pdf. [Accessed 4 October 2018].

[6] Tracy Kitten, "Why Fraudsters have shifted to Shimming Attacks," 18 November 2015. [Online]. Available: https://www.bankinfosecurity.com/blogs/banks-prevent-shimming-losses-p-1980. [Accessed 4 October 2018].

[7] Owen Wild, "Cash Trapping "Type 1" Attacks in Spain," 7 December 2016. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/brochures/ncr_security_alert_-_2016-14_cash_trapping_in_spain_0.pdf. [Accessed 7 October 2018].

[8] Owen Wild, "Transaction Reversal Fraud - Global," 09 July 2018. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/brochures/NCR%20Security%20Alert%20-%202018-06%20Transaction%20Reversal%20Fraud.pdf. [Accessed 7 October 2018].

[9] J. M. Stewart, M. Chapple and D. Gibson, "Phishing," in *Certified Information Systems Security Professional*, New Delhi, Wiley India Pvt.Ltd, 2015, pp. 617-618.

[10] Owen Wild, "Man in the Middle Network Attacks," 13 February 2015. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR-Security-Alert-2015-01-Man-in-the-Middle-Attack-in-Mexico.pdf. [Accessed 4 October 2018].

[11] Dieboldnixdorf, "Protection against the latest threat - WannaCry terminal security suite," Dieboldnixdorf, 2017. [Online]. Available: https://www.dieboldnixdorf.com/-/media/diebold/diebold-asset-library/software/dn_tss_wannacryransomeware.pdf. [Accessed 27 September 2018].

[12] Owen Wild, "Petya Ransomeware," NCR, 28 June 2017. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/ncr_security_alert_2017_06_petya_rasonware_v4.pdf. [Accessed 28 September 2018].

[13] Owen Wild, "Black Box Attacks on SelfServ ATMs in the UK," NCR, 12 June 2017. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/ncr_security_alert_2017_06_black_box_attacks_on_uk_selfserv_atms_v2.pdf. [Accessed 27 September 2018].

[14] S. Tellier, "7News Investigates: ‘Jackpotting’ Crime Wave Hits Mass. ATMs," 7 News Boston, 22 May 2018. [Online]. Available: https://whdh.com/7-investigates/7news-investigates-jackpotting-crime-wave-hits-mass-atms/. [Accessed 2 October 2018].

[15] Owen Wild, "Black Box Attacks on SelfServ ATMs in the UK," 12 June 2017. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/ncr_security_alert_2017_06_black_box_attacks_on_uk_selfserv_atms_v2.pdf. [Accessed 2 October 2018].

[16] Owen Wild , "Black Box Attacks on ATMs in Germany," 18 April 2016. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR-Security-Alert-2016-04-Black-Box-Attacks-in-Germany.pdf. [Accessed 2 October 2018].

[17] Owen Wild, "Black Box Attacks on ATMs in Italy," 14 April 2016. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR-Security-Alert-2016-03-Black-Box-Attacks-in-Italy.pdf. [Accessed 2 October 2018].

[18] J. M. Stewart, M. Chapple and D. Gibson, "Risk Elements," in *Certified Information Systems Security Professional*, New Delhi, Wiley India Pvt.Ltd, 2015, pp. 605-606.

[19] M. Nicho, "Incorporating COBIT Best Practices in PCI DSS V2.0 for Effective Compliance," *ISACA Journal,* vol. 1, no. ISACA, 2012.

[20] J. Hizver and T.-c. Chiueh, "Automated Discovery of Credit Card Flow for PCI DSS Compliance," in *30th IEEE International Symposium on Reliable Distributed Systems*, Stony Brook, 2011.

[21] N. K. Gyamfi , M. A. Mohammed , K. Nuamah-Gyambra , . F. Katsriku and J.-D. Abdulah, *International Journal of Applied Science and Technology,* pp. 102-111, 2016.

[22] F. Twum, K. Nti and M. Asante, "Improving Security Levels In Automatic Teller Machines Using Multifactor Authentication," *International Journal of Science and Engineering Applications,* pp. 126-134, 2016.

[23] P. Jindal and R. Kumar, "Analysis of Security System for ATM," in *4th International Conference on System Modeling & Advancement in Research Trends (SMART)* , Moradabad, 2015.

[24] Z. Ghafari, T. Arian and M. Analoui, "SFAMSS: A Secure Framework for ATM Machines via Secret Sharing," *International Journal of Computer Science & Information Technology,* vol. 7, no. 2, pp. 71-78, 2015.