ATM Security in the Banking Industry

Michael Mozingo
ICTN 6823 Information Security Management 601
East Carolina University
Dr. Phil Lunsford
July 21, 2016

ATM Security in the Banking Industry

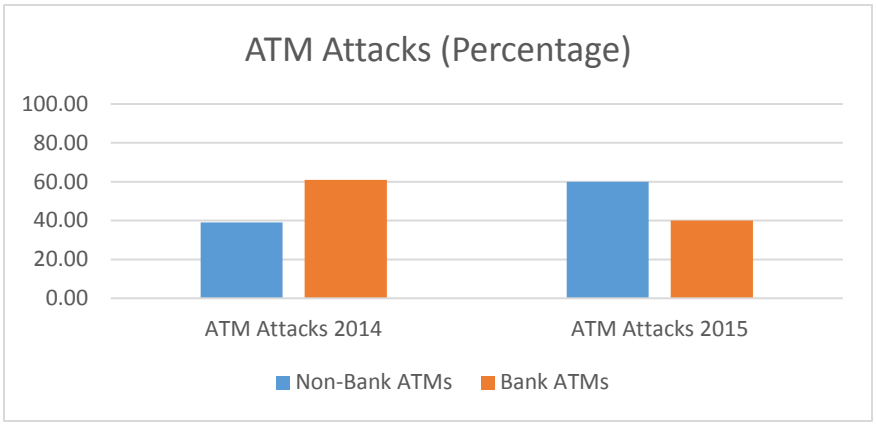
Automated Teller Machines (ATM) are used by millions of individuals every day and play an important factor in the banking footprint. Don Wetzel came up with the idea of the ATM and created the first one with the help of Tom Barnes and George Chastain. (AUTOMATED TELLER MACHINE, 1995). Chemical Bank introduced the first ATM in the United States in September of 1969 (Automated Teller Machines, 2010). Ever since the introduction by Chemical Bank, the ATM has become an important piece of technology to the banking industry as both a means for bank customers to have access to their banking information, and for banks to make money by charging fees for their usage.

In order to better understand the process of keeping ATMs secure, it is imperative to realize how they operate. The main purpose of an ATM is to allow individuals with a credit/debit card the opportunity to withdraw or deposit money into their banking accounts without physically having to enter a bank, thus, saving them time. Along with withdrawing and depositing cash, customers also have the ability to check their bank statements along with viewing any potential loans they may have with the bank who supplies the ATM. Although ATMs are limited to only a few functions, banking institutions spend a lot of time and resources in having them operational. First, the bank must research and determine where and when they are going to deploy an ATM. They must determine if the location makes sense from both a business and a customer usage standpoint. Once a location has been selected, the bank will then need to decide which company that provides and maintains ATMs they are going to use. The three main companies being used today are: Diebold, Wincor, and NCR. All three of these companies both provide ATMs and offer support incase of any issues the ATM may experience. With the number

of users increasing throughout the history of the ATM, it has become increasingly important for both banks and their customers to understand the risk involved when using these machines.

ATM Fraud Statistics

David Morrison of Credit Union Times wrote an article in which he noted the ATM Industry Association has predicted that by 2015, there will be over three million ATMs spread across the globe (Morrison, 2014). To go along with what ATM Industry Associations predicted, RBR, a London-based financial consulting firm, performed research that estimated global cash withdrawals from ATMs would increase by 7.9% per year from 2011 to 2017 (Morrison, 2014). With millions of ATMs currently in production and a high increase of withdrawals estimated for the next couple of years, it further illustrates that ATMs are still a popular means for users to access their accounts. Therefore, they must remain as secure as possible at all times. ATM fraud is a serious issue and has steadily been increasing. FICO Card Alert Services is a company that monitors ATMs for fraud. Recently, they posted an article that stated compromised ATMs increased by 546 percent between 2014 and 2015 and that the days between compromises fell from 36 days to 14 days between the same time periods (ATM Compromises, 2016). TJ Horan, vice president of fraud solutions at FICO, stated criminals are targeting non-bank ATMs in 2015 (ATM Compromises, 2016).



Horan also stated that attacks on these machines accounts for 60 percent of all comprises, compared to 39 percent in 2014 (ATM Compromises, 2016). These type of numbers

are alarming and should emphasize the importance of ATM Security to those that provide their service. Many users may think that ATM fraud only happens in bigger cities; however, the same report published by FICO Card Alert Services shows that ATM fraud in 2015 spread throughout the country instead of confined to larger cities, as was the case in 2014 (ATM Compromises, 2016).

These statistics show that everyone who uses an ATM should be mindful of their surroundings and do everything they can to keep their information as secure as possible. These statistics should also be important for the banking industry as they highlight the fact that ATM fraud is increasing tremendously.

Types of Security Concerns

ATMs, when up and operational, allow customers to obtain cash 24/7 7 days a week. With this easy access to money, individuals need to understand the important of keeping their bank information safe and staying alert while at an ATM. There are many types of security concerns when it comes to ATMs. One such concern is someone obtaining credit or debit card information and illegally withdrawing funds. The most important, yet basic, thing for users to remember is to never give out their Personal Identification Number (PIN). When using an ATM, a credit or debit card is inserted into card reader, and the user then enters their PIN to initiate the transaction (inquiry, withdraw, deposit, etc.). The reason it is so important to never give out the PIN is because once someone has the PIN, all they then need is the actual debit/card or the numbers on the card to make transactions. If they did not have the PIN but had the actual card, their options would be limited on how they could use it for their own gain. To go along with never giving out the PIN, users should also be alert to those in close proximity of the ATM in question while using it. Ensure that, when entering the PIN, the keypad is covered by either the

pin pad shield, hand, or other means. This will help prevent shoulder surfing which is the act of looking over someone's shoulder to gain information without the person's consent. Another thing to look out for when at an ATM is if a skimmer has been placed on the ATM's card reader. In order to accurately determine what a skimming device looks like, it is crucial to know what they are.

A skimmer is a device whose job is to capture data from the magnetic strip that is found on the back of a debit/credit card, and is designed to look very much like a normal card reader slot. Not only do these devices capture the information on the card, they can even capture the PIN when entered by the user (Sharma & Rathore, 2012). Victims of skimmers may not notice their information has been taken until days, weeks, or even months later because when the skimmers are placed on the machine, the individual who placed the device does not have to be nearby in order to steal the information. Instead, the individual can come back to the ATM whenever they have the chance and take their skimmer device off and replace it back with the original card reader slot or just leave it off altogether.

Although most of the physical security is focused on what customers can do to keep themselves safe from fraud, the banking institution has a responsibility to assist as much as possible. One of the easiest measures the bank can implement is to ensure their ATMs are placed in well-lit areas. This not only helps reduce the safety concerns of users, it also can help the bank make money due to their client's willingness to use the ATM as they would feel safer doing so. Another action the bank can take is to have security cameras on all ATMs. In case a person using an ATM were to be robbed, the chances of finding the criminal are increased if there are security cameras attached to the ATM. To assist in detecting skimming devices, the bank can send branch employees to ATMs to verify they have not been tampered with. An easy way to implement this

is to have branch managers check the ATM at the branch along with any that are nearby at an isolated kiosk or inside a store. These machines should be checked, at minimum, twice a month for accurate tracking.

Recent attacks on ATMs have come by the way of malware. Malware is usually installed on an ATM by using either a USB or CD-Drive (Sancho & Huq, 2016). According to the article on Trend Micro written by Sancho & Huq (2016), there are currently no statistics on malware attacks on ATMs for the United States, but the European ATM Security Team states that losses internationally were reported in 53 countries and territories, with the United States being one of the top three locations. Malware on an ATM can act similarly to a skimming device as it can be used to skim the machine for card numbers and PIN codes that are inputted by the user. Along with acting as a skimming device, malware can also dispense cash whenever the attacker chooses to run the malware (Kitten, 2013). As stated in the same article by Kitten (2013), these types of attacks are difficult to pull off and are not likely to affect branch ATMs, as they require physical access to the ATM in order to place the malware on them. Banks and credit unions should still take malware attacks seriously as most of these institutions have ATMs that are located outside of a branch with some being at a remote kiosk location that could still be vulnerable to attacks.

How the Banking Industry Can Help Prevent Fraud

Bank institutions play a major role in preventing ATM fraud and ensuring their machines are secure. These institutions, along with their customers, lose money when ATM fraud happens so it is in their interest to do as much as possible to prevent any type of fraud from happening. Not only do companies lose money, they also lose their reputation when their equipment is compromised. In this day and age, with social media, any compromise, whether big or small, can be published and seen by millions of individuals, further damaging the company's reputation.

One way in which banks can help prevent fraud is to ensure their machines are up to date with software and operating systems. It is crucial for banks to stay up to date on these issues as the ramifications could be major, such as, known exploits that have otherwise been fixed would still be exploitable causing the chances of fraud to increase. On April 8th 2014, Microsoft stopped supporting Windows XP. Jose Pagliery (2014) wrote an article for CNN stating there were an estimated 95% of American ATMs that were still running on Windows XP. With Microsoft ending support for Windows XP, banks had to update the operating system on their ATMs to Windows 7 in order to keep receiving updates and support from Microsoft. According to Pagliery (2014), experts estimated it could cost between $1,000 and $3,500 per machine to update the software and operating systems. Fortunately, banks were able to cut deals with Microsoft to extend support for Windows XP which allowed them more time to update their machines (Pagliery, 2014).

Another way banks can help prevent ATM fraud is to constantly monitor the machines 24/7. Banks can use outside companies such as Securitas, to assist them in actively monitoring these machines and report any issues that may arise. Companies that specialize in monitoring can provide expertise and knowledge on security risks that banks may not necessarily have an understanding on. According to Securitas, they provide multiple services including: intrusion alarm monitoring, arm and disarm supervision, ATM skimming alert monitoring, video alarm verification, and many more (Security Monitoring, n.d.). These types of monitoring can prove to be extremely valuable for banks as they can help prevent fraud from happening by signaling an alarm to the company if someone has entered the ATM without authorization. They can also help assist in identifying those who may have committed fraud by use of surveillance cameras.

Future of ATM Security

With the increase in ATM fraud and the fear from banking institutions of losing customers and their reputations, banks will be looking to further secure their machines. Technology is constantly changing and the banking industry can use these changes in technology to increase the security of their ATMs.

One possible avenue of ATM security that is beginning to see more research in is biometric usage. Kulkarni, Madki, and Mapari (2016), conducted a research paper in which they listed some of the ways biometrics can be used to secure ATM transactions along with some of the advantages of using the technology. Merriam-Webster's dictionary describes biometric as "the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity" (Biometrics, 2016). Types of biometrics mentioned in the research paper include Physiological, Geometry, and Behavioral techniques. Physiological technique use hand and finger prints while the Geometry technique uses the eyes retina and iris along with the wrist. Behavioral technique uses voice, signature, typing and pointing (Kulkarni, Madki, and Mapari, 2016). Knowing what biometrics is along with the different types that could be used, it becomes easy to see how this type of technology can greatly benefit ATM security. Imagine when using an ATM, instead of entering a PIN, the user places their hand or finger on a scanner which will then verify the user's identity and allow them access to their banking accounts. The same can be done for the user's eye or voice. Another benefit of implementing biometrics is that they lock down the internal systems of an ATM making the electronic points of entry unavailable to attackers (Carnesi, 2014). As an extra layer of security, biometrics can be used alongside

traditional PIN entries to produce a more secure two-factor authentication process (Gupta, Rao, and Upadhyaya, 2004).

Banks are starting to introduce card-less ATMs that, as the name suggest, uses a card-less system for users to access their accounts. Brian Barrett of Wired.com wrote an article that discusses how your phone will replace your wallet while at an ATM. Instead of using a credit/debit card to initialize the transaction, the user uses their phone. This technology has only recently seen progress in the United States, but Spain has been using card-less ATMs since 2011 (Barrett, 2016). BMO Harris Bank implemented these ATMs in March of 2015 and JPMorgan Chase has announced they will be providing thousands of machines that will only require a smartphone to allow its users to withdraw from their accounts (Barrett, 2016). There are different way to use this type of card-less system. For example, BMO Harris Bank requires customers to install the banks app and put how much they are looking to withdraw in the app. Once the user arrives at the ATM, they tap an icon on the screen, place their smartphone so that the ATM can scan a QR code which will then allow for them to withdraw the cash they requested within the app (Barret, 2016). According to Barrett (2016), Chase will be, at least initially, offering the same type of system by having customers install their app to acquire a seven-digit access code that they would then use at the ATM, thus eliminating the need for a credit/debit card. In its current state, card-less ATMs are not necessarily meant to be a quicker way to use an ATM as they force users to access an app before going to the ATM, however, it does provide a more secure experience by eliminating the need for a credit/debit card. Chase, however, will be producing ATMs that will be equipped with Near Field Communication (NFC) that will allow the ATM to communicate directly with the customer's smartphone (Barrett, 2016). These transactions will be similar to how Apple, Android, and Samsung pay currently operate in that

the ATM will recognize the smartphone and the user will have to provide a password or fingerprint on their phone to successfully complete the transaction.

EMV chip cards could play a key role in increasing security at ATMs. In October 2014, President Obama issued an executive order which made it mandatory for payment card issuers to begin implementing their cards with EMV microchip technology by October 2015 (Angeles, 2015). EMV stand for Europay, MasterCard, and Visa and it is a credit card standard that enhances the security of in-person card transactions (Angeles, 2015). Credit and debit cards that utilize this technology have a chip placed on the card themselves. These cards allow for information to be stored on the chip instead of the magnetic strip of the card, offering superior security (Angeles, 2015). What makes these EMV chip card different than traditional cards are the way in which they are used. EMV cards are dipped into the card reader rather than swiped (Angeles, 2015). Cards that are swiped use the magnetic strip and the data can be reused multiple times by hackers, while EMV cards produce a unique code for each use and can only be used that one time (Angeles, 2015). Part of the move to EMV is that as of October 1, 2016, manufacturers will assume financial liability for fraudulent transactions for chip enabled MasterCards, and in 2017, Visa will do the same (ATM EMV, 2016). What this means is, companies that have not made their ATMs available to accept EMV credit/debit cards, can be held responsible for any fraudulent charges that may happen at their machines. Although this move will enhance security at ATMs, the move has been slow. Per Business Insider's website, roughly 35% of US ATMs will have made the needed upgrade by October 2016 (ATM EMV, 2016). Business Insider (2016), notes that the slow response to upgrading these machines can be contributed to the high cost with each upgrade costing between $300 and $3,000.

Conclusion

ATMs will continue to be a key component in the banking industries footprint as they have been since their introduction. Banks and credit unions with have to diligently work on keeping these machines as secure as possible to fight against current threats along with new ones that may occur in the future. Attacks on ATMs will not stop anytime in the foreseeable future as criminals will continue to see them as an easy and quick way to obtain money. The banking industry is known to be stuck in their ways and not necessarily looking to embrace new technology as soon as it is available. Going forward, this type of thinking will need to change as newer technology is making it easier for criminals to access ATMs and steal from both users and the banks themselves. With new technology, such as, skimming devices and potential malware attacks, attempt to breach ATMs are sure to increase. Therefore, it is vital that both those in the banking industry and those that provide ATMs (Diebold, NCR, and Wincor) continue to work collaboratively to ensure they stay up to date on protecting their devices. Not only will doing so protect their customer's information, but it will also keep their reputation intact.

References

Angeles, S. (2015, September 30). EMV: What Small Merchants Need to Know. Retrieved July 12, 2016, from http://www.businessnewsdaily.com/7859-emv-technology-small-businesses.html

ATM Compromises in US Jumped Six-Fold in 2015, FICO Reports. (2016, April 08). Retrieved May 26, 2016, from http://www.fico.com/en/newsroom/atm-compromises-in-us-jumped-six-fold-in-2015-fico-reports-04-08-2016

ATM EMV migration in the US is moving slowly. (2016, July 11). Retrieved July 12, 2016, from http://www.businessinsider.com/atm-emv-migration-in-the-us-is-moving-slowly-2016-7

AUTOMATED TELLER MACHINE CELEBRATES 30 YEARS; NATIONAL MESUEM OF AMERICAN HISTORY ADDS AN ATM TO COLLECTION. (1995, September 20). *PR Newswire*, p. 920DC005. Retrieved from http://go.galegroup.com.jproxy.lib.ecu.edu/ps/i.do?id=GALE%7CA17440499&sid=summon&v=2.1&u=nclive&it=r&p=STND&sw=w&asid=1bd1674de1727a84ec9841f52466c017

Barrett, B. (2016, January 28). Your Phone Will Replace Your Wallet at the ATM, Too. Retrieved July 07, 2016, from http://www.wired.com/2016/01/cardless-atms/

Biometrics. 2016. In *Merriam-Webster.com*. Retrieved July 7th, 2016, from http://www.merriam-webster.com/dictionary/biometrics

Carnesi, K. (2014, April 24). THE FUTURE OF ATM SECURITY. Retrieved July 7, 2016, from https://www.linkedin.com/pulse/20140424182524-203717372-the-future-of-atm-security

*Gupta, M., Rao, R., & Upadhyaya, S. (2004). Electronic banking and information assurance issues: Survey and synthesis. *Journal of Organizational and End User Computing, 16*(3), 1-21. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/199922626?accountid=10639

Kitten T. (2013, October 14). ATM Malware: Sign of New Trend? BankInfoSecurity. Retrieved June 30, 2016 from http://www.bankinfosecurity.com/atm-malware-growing-concern-a-6143/op-1

*Kulkarni, R., Madki, M., & Mapari, T. (2016). CARD-LESS ATM SYSTEM. *International Education And Research Journal, 2*(4). Retrieved from https://issuu.com/thewriterspublication/docs/49-rushikesh_kulkarni

Morrison D. (2014, July 28). 3 Million ATMs Worldwide By 2015: ATM Association. Credit Union Times. Retrieved July 5, 2016 from http://www.cutimes.com/2014/07/28/3-million-atms-worldwide-by-2015-atm-association

Pagliery, J. (2014, March 4). 95% of bank ATMs face end of security support. Retrieved June 15, 2016, from http://money.cnn.com/2014/03/04/technology/security/atm-windows-xp/index.html

Sancho D, Huq N. (2016, April 12). ATM Malware on the Rise. TrendLabs Security Intelligence Blog. Retrieved June 30, 2016 from http://blog.trendmicro.com/trendlabs-security-intelligence/atm-malware-on-the-rise/

Security Monitoring. (n.d.) Retrieved June 19, 2016 from http://www.dieboldsecurity.com/services/security-monitoring

*Sharma, N., & Rathore, D. S. (2012). ANALYSIS OF DIFFERENT VULNERABILITIES IN AUTO TELLER MACHINE TRANSACTIONS. *Journal of Global Research in Computer Science*, *3*(3), 38-40. Retrieved May 22, 2016, from http://jgrcs.info/index.php/jgrcs/article/view/340/277