Global Information Assurance Certification Paper

Automated teller machine theft is a major problem. Although banks do not publish their losses due to computer crime, A BAI Global study estimates one ATM crime is committed for every 2 million transactions, or about 5,500 crimes a year. The American Bankers Association puts the number at an even lower one crime for every 3.5 million transactions, or about 3,000 a year[1]. With consumers becoming more dependent on ATMs and the proliferation of ATM debit cards, computer crime in this area is more likely to increase. Banks will have to find better methods to eliminate unauthorized use through hardware or software solutions, while keeping security costs down. The purpose of this case study is to explain how ATM fraud occurs, and possible solutions banks can implement to prevent such loss.

Automated teller machines (ATMs) are a part of most of our lives. The major appeal of these machines is convenience. ATMs allow customers access to get cash, pay bills, purchase or sell securities, or make deposits twenty-four hours a day. Customers access their bank accounts through a plastic bankcard. This card has a magnetic strip on the back containing a password and relevant account information. ATM technology has virtually remained the same over the last several decades, with a few minor changes like color touch-sensitive screens and voice-activated commands for the visually impaired. Citibank, which pioneered a full ATM network 23 years ago, now has a worldwide network covering offices in over 100 countries around the world. With so many machines available to account holders, it's no wonder that illegal users take advantage of this technology.

Most banks use input validation techniques (batch totals, format checks, reasonableness checks, transaction validation) and audit trails are used to verify that the transaction came from a valid bankcard in an authorized ATM center. These features do not eliminate the need for users to write down passwords; they just ensure that the data transmitted follows certain guidelines, that requests such as cash withdrawals are made within reasonable limits, that money is transferred to the proper account, and so forth. These features only ensure that certain procedures are followed, and cannot tell whether the person with the card and password is authorized to use it. To stop a criminal, who has a stolen ATM card and password, system security measures must be improved to identify the person using the card.

Over the past decade, criminals have used social engineering techniques to commit fraud. There are two common scams: card withholding, and ATM deposit fraud.

ATM deposit fraud is a common occurrence that targets a bank and the victim. The thieves open new ATM accounts at a bank, then take the newly acquired ATM card and make fraudulent deposits (mostly on Friday nights after the bank closes) with fraudulent checks that cannot be processed until the following Monday. Then on Saturday morning, the thief withdraws cash for the deposited checks knowing that the check will bounce. The bank will identify the error and close the account, limiting the loss to less than $3000 in most cases. Once gang succeeded in defrauding banks for over $800,000 over the course of two years before they were apprehended and proscecuted[2]. Although banks like Citibank used a simple countermeasure of allowing the customer to withdraw a small

portion of the deposited check and keeping the total of the deposits unavailable until the checks clear, yet this attack is still being performed on other banks that have not closed this vulnerability.

Card withholding is a crime that requires a lot of social engineering, and a 'spotter' to gain the two items necessary to defraud the consumer: their ATM card, and PIN. The thieves usually use something to jam an unsuspecting customer's card in the ATM machine then try to 'help' their victim remove the card. After several failed attempts, they sympathize with the target, and even suggest they type their PIN in several times in the hopes that the ATM will release the card. While this is happening, an accomplice (the spotter) is nearby to see the PIN being entered. After the frustrated victim leaves without the card, the thieves use a nail file to extract the card, and withdraw cash using the PIN they just observed. Most ATM machines are designed to not take the card in completely for this reason, and some banking centers are equipped with 24-hour surveillance and access to local police if a suspected scam is in progress[3].

Another more sophisticated crime used a Fujitsu model 7020 automated teller machine in the Buckland Hills Mall in Hartford, Connecticut. The criminals installed a specially programmed machine in the mall to record the card information, collect the PINs from the unsuspecting customers, and let the system inform them that the transaction they requested could not be processed. Days later, the gang collected the information and made bogus ATM card which were then used to withdraw money from the victim's accounts from ATMs in Manhattan. The criminals were caught when the use of the counterfeit ATM cards was correlated with the surveillance cameras[4].

A more recent vulnerability although not widespread at this time is a technique called skimming. The crime uses a black box the size of a Palm Pilot, with a slit down the front and bits of Velcro tape on the back. Called a "skimmer," the device can read and store the data embedded within a charge card's magnetic stripe — not only the name, number and expiration date that appear on the card's face but also an invisible, encrypted verification code that is transmitted electronically from merchant to card issuer to confirm a card's validity at the point of sale. By copying that code, the counterfeiter has all the data needed to create a perfect clone of the charge card. This method was recently used to defraud 100+ American Express cardholders of nearly $500,000 last summer[5], and the technology is portable enough to be used in a modified ATM in a supermarket or other public area. This type of fraud is usually not caught until the customer receives their monthly statement 30 days after the transaction occurs. If the victim does not read their statements carefully, this type of attack will be hard to detect because it compromises the authentication of the customer transaction and the confidentiality of the customer's information on the card.

Many of the methods used to defraud consumers and their banks can be minimized through the use of biometrics devices, or enhanced ATM security software.

Biometrics devices have been available for over a decade, and the cost of the technology

has significantly dropped over the years. Companies like Sensar Corp (now Identix Technologies) are using biometrics devices to authenticate customers by iris scans at ATMs in Europe. Texas's Bank United was the first US bank to implement iris recognition at ATM's and the first bank anywhere to use the technology in the single-factor mode — without PINs, passwords, or cards. Using an IrisCode® record, a digitized 512-byte representation of the feature-rich iris, or colored part of the eye, the system can authenticate the identity of individuals with greater accuracy than any other method, to help eliminate fraud. The system requires no contact and minimal cooperation to function[6].

Another security measure that is effective in alerting the police of an ATM robbery are the use of software such as Zi-Cubed's SafetyPIN product. The SafetyPIN system, when implemented at a bank, will allow a customer who may be in the middle of a robbery to discreetly alert the police by using a secondary PIN. The alternate PIN will still authorize the ATM to dispense cash, but the system will alert the police and direct them to the ATM center where the suspect robbery is occurring[7].

Even though user-supplied passwords will eliminate many of the vulnerabilities inherent in a PIN-based ATM system, banks still have to improve surveillance, fraud detection and procedures that involve law enforcement sooner to minimize ATM crime. The second part to minimizing fraud is the most important step banks should take to reduce this type of crime - customer education. Most banks make an attempt at warning account holders of the ways this crime happens, but it is not good enough. Banks should post warnings next to ATMs machines telling customers not to give their card to anyone else except bank officials, and pamphlets should be mailed out periodically with account statements. The minimal cost of better customer education will reduce the millions of dollars lost through ATM fraud, while maintaining the balance between the cost of security and the cost of a financial loss due to fraud.

[1] "Crime continues to dog ATM industry" February 19, 1999. URL: http://www.atmmagazine.com/news_story.htm?i=670

[2] *Bailey, Karen. "U.S. Department of Justice Office of the U.S. Attorney, District of Minnesota Press Release".* October 18, 2000. URL: http://www.usdoj.gov/usao/mn/press/econ/norris.htm

[3] 'Where ATM con artist "The Raven" strikes next, nobody knows'. September 18, 1998. URL: http://www.atmmagazine.com/news_story.htm?i=414

[4] Schneier, Bruce. "Secrets and Lies: Digital Security in a Networked World". John Wiley & Sons, Inc.New York, NY 2000. p. 46-47.

[5] Shannon, Elaine. "A New Credit-Card Scam" Time Europe, July 10, 2000 vol. 156 no. 2. URL: http://www.time.com/time/europe/magazine/2000/0710/creditcard.html

[6] Iridian Technologies Iris Recognition ATMs. http://www.iridiantech.com/questions/q4/case_studies.html

[7]Zi-Cubed's SafetyPIN system and product description. URL: http://www.zicubedatm.com/html-3.html

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event