Feature

Henry Santiago is a recent graduate of East Carolina University (Greenville, North Carolina, USA) with a Bachelor of Science in information and computer technology and a minor in business administration. Santiago interned with the Department of Technology for Cumberland County Schools in North Carolina, USA, in 2015.

ATM Risk

From January to 9 April 2015, the number of attacks on debit cards used at automated teller machines (ATMs) reached the highest level for that time frame in the last 20 years.[1] Rather than attempting to physically break into an ATM, criminals nowadays are using more advanced ways of stealing money and data. The main methods today's criminals are known for using include ATM skimming, ATM hacking and radio frequency identification (RFID) credit card skimming.

ATM skimming is an action in which criminals use hidden electronics to steal personal information from ATM users. Hidden cameras, malicious keypads and counterfeit card readers are the primary devices criminals use for skimming. When it comes to hacking ATMs, criminals can easily purchase used ATMs online, some of which retain a list of users and their personal data within the machine's memory, which can be accessed without having to provide credentials. Even when ATM users are not using an ATM, their personal banking information can still be stolen by criminals skimming RFID credit cards. Although modern RFID credit cards use encryption and other advanced security measures, criminals used to be able to easily use a homemade skimming device that could wirelessly obtain the credit card data without physically touching it.[2]

Some simple ways ATM users can keep their money safe and protect their bank account information include visually and physically examining the credit card reader and the keypad to ensure that a malicious device is not mounted on the machine. A user can also check on and around the ATM for cameras that may be used to record personal identification numbers (PINs). To be safe, users should consider covering the keypad as they enter their PIN. ATM users should also develop the habit of monitoring their bank account online daily to watch for transactions that were never made. And finally, users can protect their money and bank account information by avoiding ATMs that are located in dark or hidden areas.[3]

There are also technology-based ATM security measures. The first kind of technologically advanced protection is called access protection. Access protection guards ATMs from unauthorized access through the operating system login processes. A major feature of access protection is known as operating-system hardening, which helps to minimize the system's vulnerabilities by eliminating as much security risk as possible when there is a removal or disabling of all nonessential operating system components and services. However, the most simple and common feature of access protection is using PINs for a user's credit and debit card account access.

Intrusion prevention systems (IPS), in general, are a combination of security technologies, policies and rules designed to protect self-service machines against unauthorized software installations.[4] Specifically, IPS can protect ATMs against malware attacks such as Trojans, worms and even zero-day attacks. In addition to this, IPS can also protect ATMs from the manipulation of system components that may attempt to force unauthorized cash withdrawals and steal personal data from users. Criminals have been known to connect to ATMs with a Universal Serial Bus (USB) cord and hack into them to change the machine's software and, later, steal sensitive information.

The third type of ATM security is called hard-disk encryption. This kind of encryption is used to encrypt the entire hard disk of the machine, which makes data stored in the ATM inaccessible unless a specified authorization process is executed. Hard-disk encryption protects data from theft or misuse when an ATM is switched off while being decommissioned and during unauthorized booting. However, unlike traditional computer disk encryption, which requires passwords or security tokens, ATM hard-disk encryption uses the PIN pad, card reader and dispenser module. If the hard disk or the entire ATM is removed from its authorized location, the network will disable the terminal's ability to authenticate. In other words, there will no longer be access to the hard disk.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal),* find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

The fourth kind of ATM security available is known as optical security guards. These security guards are made up of optical sensors that monitor ATMs and are used to prevent illegal actions, including skimming and trapping, from taking place. Optical security guards, including the customer panel camera and the card entry slot cameras that are integrated into the ATM, use smart-image analysis software that is able to decide whether a transaction is normal or malicious. If the ATM detects any tampering, an alarm will be triggered and, if necessary, will stop all further transactions immediately. The immediate response time of the optical security guards reduces the risk of fraud or physical damage to the ATM.

Similar to optical security guards, video surveillance cameras are also used to continuously monitor ATM transactions. Video surveillance cameras are usually mounted on and near ATMs to record everything that is happening near the machine. However, unlike the optical security guards, regular video surveillance cameras do not have the ability to automatically stop a malicious transaction. But if a security guard is currently viewing the surveillance feed, he/she can take action to prevent any malicious attacks. After-hours at a bank when there is no one monitoring surveillance cameras, the cameras will still be able to capture any malicious activity, which will be recorded for later viewing. These cameras can be helpful by recording any malicious transactions and can even help identify the criminals involved in the crime.[5]

Banks in Central and South America, Africa and the Middle East are currently moving toward biometric technology for ATMs. Biometrics is a rapidly advancing field that focuses on identifying a person based on his/her physiological or behavioral characteristics. Fingerprinting technology, in particular, can be much more reliable in authenticating ATM users than current methods used around the world. However, certain regions, the US for example, have not yet implemented the use of fingerprinting technology for ATMs because of consumer liability for fraudulent charges and because of the cost of adopting this new technology.[6] Additionally, concerns regarding consumer privacy are another major obstacle when it comes to moving forward with adopting this technology for ATM transactions. Furthermore, fingerprinting technology is also hampered by the fact that fingerprints can easily be lifted and replicated. Criminals can lift and preserve fingerprints with a special kind of dust and tape. Another way that criminals can collect fingerprints is to photograph them with high-resolution cameras.[7]

Thus, the most secure biometric technology today uses an iris scan (eye scanner) that is based on more than 2,000 measurement points. Like fingerprint scanning technology, iris scanning technology is also costly to implement. Nevertheless, iris scanning technology remains an option for the future of ATM security.[8]

As the number of ATM users continues to grow, so does the security risk. But as security risk grows, new technologies will continue to be created to fight these cybercrimes. However, all ATM users must continue practicing safe and smart methods of making transactions on their own to avoid having their credit card numbers, bank account information or money stolen.

ENDNOTES

[1] Sidel, R.; "Theft of Debit-Card Data From ATMs Soars," *The Wall Street Journal*, 19 May 2015, *www.wsj.com/articles/theft-of-debit-card-data-from-atms-soars-1432078912*

[2] Fenlon, W.; "How Does ATM Skimming Work?" HowStuffWorks.com, 8 November 2010, *http://money.howstuffworks.com/atm-skimming.htm*

[3] McGoey, C.; "ATM Machine Security," CrimeDoctor.com, *http://crimedoctor.com/atm.htm*

[4] Wincor Nixdorf, "Terminal Security," *www.wincor-nixdorf.com/internet/site_AT/EN/Products/Software/Banking/ProClassicEnterprise/Security/PCETerminalSecuity/HardDiskEncryption/HardDiskEncryption_container.html?nn=1181148*

[5] O'Neil, E.; "ATMs Use Biometrics to Combat Fraud," About.com, *http://banking.about.com/od/securityandsafety/a/biometricatms.htm*

[6] National Forensic Science Technology Center, *A Simplified Guide To Fingerprint Analysis*, 2013, *www.crime-scene-investigator.net/SimplifiedGuideFingerprints.pdf*

[7] *Op cit,* O'Neil

[8] Scarfone, K.; "The Basics of Network Intrusion Prevention Systems," *Tech Target*, 2015, *http://searchsecurity.techtarget.com/feature/The-basics-of-network-intrusion-prevention-systems*