**Threat Modeling of an ATM**

**Student**: Patrick Walsh

**Date**: 4/18/2021

**School**: University of Maryland Global Campus

**Course**: SDEV 360 7380

**Professor**: Dr. Alla Webb

**Architectural components of an ATM**

Automatic Teller Machines (ATM) allow a user physically present at the device to perform various financial transactions, including checking the balance of a checking or savings account, making cash withdrawals and deposits, and transferring funds (Agarwal, 2021). In order to perform these actions, the user must enter a debit card into the ATM’s card reader and enter a Personal Identification Number (PIN) through the keypad. The physical components of an ATM generally consist of two input components and four output components (Agarwal, 2021). The input components are the card reader and keypad, and the output components consist of a speaker, display screen, receipt printer, and cash dispenser (Agarwal, 2021). The ATM also requires a network connection in order to send user inputs to a bank or financial transaction center and return results such as showing account balance or dispensing money (Agarwal, 2021). At each of these components exists the possibility for threat vulnerabilities which could be exploited by malicious actors, but this paper will focus on the card reader, keypad, cash dispenser, and network components.

**Attack number 1: card reader and keypad**

One of the most common attack points of an ATM is the card reader and keypad. Criminals will target debit cards which users insert into the ATM in order to steal the card information and user PIN (PCI Security Standards Council, 2013). This kind of attack can be done without the need for highly sophisticated skills or equipment, requiring only a small pinhole camera and card reading device called a ‘skimmer’ (PCI Security Standards Council, 2013). The skimmer is used to capture card information from the user when he or she inserts a debit card into the ATM card reader and the camera is used to capture the user’s PIN as they enter it into the keypad (PCI Security Standards Council, 2013). This stolen information is used by criminals to create counterfeit cards used to conduct fraudulent transactions from anywhere in the world (PCI Security Standards Council, 2013).

**Suggested mitigation**

Users can take steps to guard against having their accounts compromised by skimmers and hidden cameras. Since the cameras are so small, it may be nearly impossible to detect their presence, so to be safe, the user should cover the keypad with the other hand to prevent unwanted eyes from seeing their PIN. Additionally, users should look for signs of tampering on the ATM card reader. Criminals may have installed skimmers by removing pieces of the card reader device, so users should watch for signs of abuse or alteration. Companies can also conduct periodic sweeps of their ATMs to look for signs of tampering, as well as install secondary cameras to record and monitor ATM users. This can help deter criminals from installing malicious equipment in the first place if they know that their actions are being recorded on video.

**Attack number 2: cash dispenser**

Another more traditional point of attack is at the cash dispenser where criminals remove cash from the ATM by brute force. While this type of physical attack is not as common today, ATMs can still be targeted in this violent way (PCI Security Standards Council, 2013). This kind of attack requires little to no technical knowledge and could be carried out by low-level criminals. Due to the crude and forceful nature of this attack, the perpetrator exposes him or herself to discovery since physically breaking into an ATM’s cash dispenser will likely create significant noise and could easily be noticed by nearby onlookers.

**Suggested mitigation**

Even though this kind of attack is not as common today, criminals, especially low-level or opportunistic ones, will still conduct brute-force entry attacks to steal cash straight from the ATM. To prevent this, ATMs should be reinforced with strong lock boxes to make infiltration difficult. The ATM can also be rigged with a security alarm to alert law enforcement if the cash dispenser is opened without authorized approval. A silent alarm may be of use so that the criminal does not realize that police have been informed during an attempted break-in. However, loud alarms which alert potential nearby onlookers have the advantage of creating witnesses by alerting people nearby that the ATM is being robbed. Finally, ATMs should have cameras that monitor and record all users so that criminals can be identified if they break into the ATM.

**Attack number 3: network connection**

Criminals have started to employ more sophisticated methods of attack, targeting the network connection of the ATM. Attackers can install malware onto the network drives of the ATM, either through a physical connection like a USB port, or by penetrating the network (PCI Security Standards Council, 2013). Once malware is installed, the attacker can capture card information and transaction data. This type of attack can be combined with Attack number 1 to steal user’s sensitive information or be done entirely remotely (PCI Security Standards Council, 2013). Aside from installing malware onto the network, an attacker could also use a network traffic sniffer to capture transactions between the ATM and a remote processing center which handles requests by the user (Positive Technologies, 2018). The attacker must connect to the same network as the ATM in order to carry out this kind of attack, but once they are on the network it is relatively easy to capture the network traffic because the ATM traffic is nearly always transmitted in plan, unencrypted cleartext (Positive Technologies, 2018).

**Suggested mitigation**

The network should have strong security so that attackers cannot infiltrate the ATM’s network. This means having a strong password and limitation on the number of login attempts before being locked out to prevent brute force password guessing. Network administrators may also consider using a device whitelist to allow only approved devices onto the network. However, one of the most critical actions companies could do to prevent network traffic from being intercepted and exploited is to encrypt the network traffic. Sensitive information like bank account details, account balances, and user information should never be sent in plain, unencrypted cleartext.

**References**

Agarwal, T. (2021, January 2). *Automated Teller Machine: Block Diagram, Types & Its Working*. ElProCus - Electronic Projects for Engineering Students. https://www.elprocus.com/automated-teller-machine-types-working-advantages/

Open Web Application Security Project (OWASP). (n.d.). *Application Threat Modeling | OWASP.* https://owasp.org/www-community/Application\_Threat\_Modeling

PCI Security Standards Council. (2013, January). *Information Supplement: ATM Security Guidelines*. Pcisecuritystandards.Org. https://www.pcisecuritystandards.org/pdfs/PCI\_ATM\_Security\_Guidelines\_Info\_Supplement.pdf

Positive Technologies. (2018, November 14). *ATM logic attacks: scenarios, 2018*. Positive Technologies Security. https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/