**Threat Modeling**

Benjamin M. Brandhorst

University of Maryland Global Campus

SDEV 360 6380 Secure Software Engineering

Professor Kevin Woodson

February 16th, 2020

**Security Objectives – Protect both money and account information**

The objective of this threat modeling procedure is to reduce the risk of a malicious actor unlawfully gaining access to money within the Automatic Teller Machine (ATM). Additionally, we want to protect customer bank account information for all users of this ATM. Finally, we must protect the information stored on the bank servers.

**Application Overview – High level architecture**

**A close up of text on a white background

Description automatically generated**

Figure 1 – High level architectural diagram of our Automatic Teller Machine (ATM)

**Identifying Threats – Threat Overview**

|  |  |  |
| --- | --- | --- |
| Threat Type | What Attacker Does | Notes |
| Spoofing a person | Accesses another customer’s bank account | This can be combined with the skimming attacks to access customer account funds. |
| Tampering with the ATM hardware | Redirects the flow of data to locally installed black box | The ATM could be modified to bypass the actual bank server. Instead a locally installed black box is used to always answer yes to the funds availability check that is done when customers try to withdraw cash. |
| Tampering with the card reader | Skims bank card information | A small card skimmer can be placed over the actual ATM card reader to skim the card information of every customer that uses the ATM. |
| Tampering with the keypad | Skims Personal Identification Numbers (PIN) | Attackers can use a camera aimed at the keypad or an overlay on top of the keypad to skim PINs. |
| Information disclosure against a data flow | Redirects traffic to enable reading data on the network | This includes session hijacking like a man in the middle attack where the communications between the ATM and bank servers are monitored or modified. |

Table 1 – Threat Overview [Table format sourced from (Shostack, 2014, p. 64)]

**Mitigation Strategy – Preventing Exploitation**

**Spoofing a person**

It is a given that our ATM requires both a bank card and a PIN in order to access customer account information. It is impossible to protect against the possibility that a bank card along with its PIN could fall into the wrong hands. If a malicious actor can secure both of these

things, our only defense against them draining a customer bank account is to set limits on the amount of cash that can be withdrawn each day. We can also ensure that our ATM includes a camera and the ATM logs include timestamps, so it is possible to match up video with all of the transactions.

**Tampering with the ATM hardware**

Black box attacks often use the cable to the cash dispenser to connect single board computer like a Raspberry Pi and issue commands to the dispenser. This allows malicious users to dispense the cash within the ATM without accessing accounts. These types of hardware tampering can be mitigated against through the use of physical authentication between the Operating System (OS) and the peripherals connected to the ATM. Additionally, the communications between the OS and the peripherals should be encrypted to prevent interception. Finally, all security events should be logged and monitored ("ATM logic attacks: Scenarios, 2018," 2018).

**Tampering with the card reader**

Now that we know how easily bad actors can attach devices to an ATM to skim the card information, there are a couple of practical steps we can take the mitigate against this type of attack. First and foremost, we can design the ATM card reader in such a way that makes it extremely difficult for an attacker to attach a skimmer to it. Additionally, we can include sensors in the card reader that will take the ATM out of service if covered by anything like a skimmer ("Anti-skimming protection for your ATM," n.d.).

**Tampering with the keypad**

Similar to our card reader protections, the keypad tampering mitigation strategy will include design modifications that make it difficult for a bad actor to place another keypad over it.

Additionally, we can include a sensor that cannot be covered in the actual keypad. This will take the ATM out of service if something is placed over it for a set length of time.

**Information disclosure against a data flow**

We can mitigate against network tampering with a three-part solution. 1.) Ensure that all data between the ATM and the bank servers is encrypted. 2.) Ensure that our Virtual Private Network (VPN) protection is implemented properly. This entails ensuring that there is no easy method of disabling the VPN and that the VPN client is secured within the ATM itself. 3.) Use message authentication codes in all transaction requests and responses ("ATM logic attacks:

Scenarios, 2018," 2018).

References

Anti-skimming protection for your ATM. (n.d.). Retrieved from https://www.cumminsallison.com/us/en/products/atm/anti-skim

Anti-Skimming Protection for Your ATM. (n.d.). Retrieved from https://www.cumminsallison.com/us/en/products/atm/anti-skim

Application threat modeling. (n.d.). Retrieved from https://owasp.org/www-community/Application\_Threat\_Modeling

ATM logic attacks: Scenarios, 2018. (2018, November 14). Retrieved from https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/

Microsoft. (2017, August 17). Mitigations - Microsoft threat modeling tool - Azure. Retrieved from https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-mitigations

Shostack, A. (2014). Threat modeling: Designing for security. Hoboken, NJ: John Wiley & Sons.