Secure Software Design

Daniel M Beck

UMGC – SDEV-360

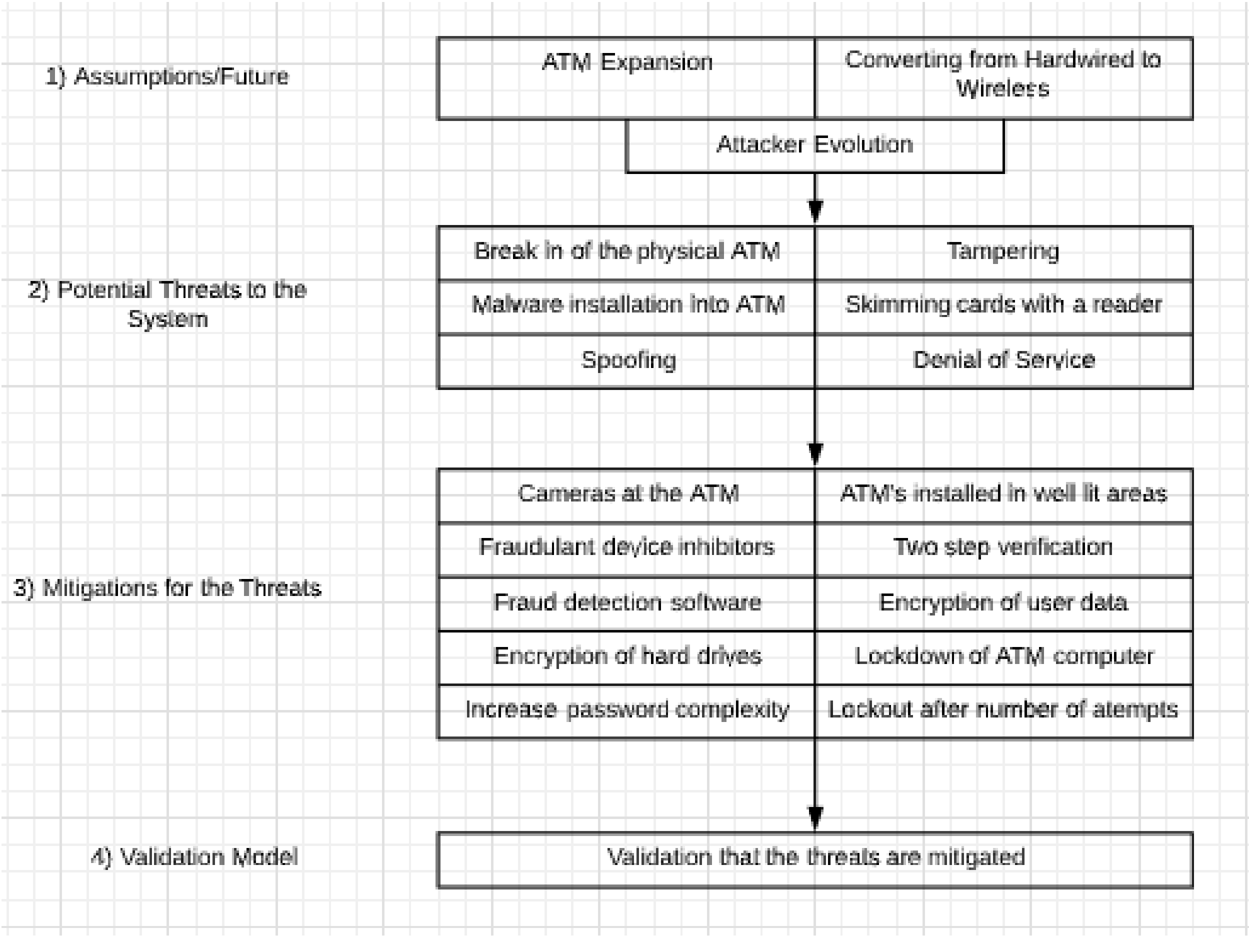
July 21, 2020

Secure Software Design

Introduction

In designing an ATM structure, threat modelling is important as “works to identify, communicate, and understand threats and mitigations within the context of protecting something of value” (Application Threat Modeling). With ATM’s and banking in general, there are many risks, that if exposed, can be devastating to the users and business, making it imperative that threat modeling be completed thoroughly.

High-Level Architectural Design


1) Assumptions/Future
ATM Expansion
Converting from Hardwired to Wireless
Attacker Evolution
2) Potential Threats to the System
Break in of the physical ATM
Tampering
Malware installation into ATM
Skimming cards with a reader
Spoofing
Denial of Service
3) Mitigations for the Threats
Cameras at the ATM
ATM's installed in well lit areas
Fraudulant device inhibitors
Two step verification
Fraud detection software
Encryption of user data
Encryption of hard drives
Lockdown of ATM computer
Increase password complexity
Lockout after number of atempts
4) Validation Model
Validation that the threats are mitigated

Assumptions That Can Be Checked or Challenged

There are a multitude of assumptions that can be may that may lead to the creation of more threats that need to be mitigated. Some of these include:

- Expanding areas where ATMs will be installed
- Transition from hardwired ethernet connection to wireless connection
- Attackers will always be evolving

Potential Threats to The System

Risk analysis is geared towards assessing risks that the system faces. “Risk analysis can be implemented as an iterative process where information collected and analyzed during previous assessments are fed forward into future risk analysis efforts” (Peterson, Hope, & Lavenhar, 2013). There are many risks that are encountered with the physical ATM including:

- Physical security of the ATM
- Protecting the computer system in the ATM from malware
- Card and currency fraud on the machines and the skimming attacks
- Machine tampering
- Accessing and using another user's credentials (Spoofing)
- Denial of Service which denies access to valid users, such as by making a web server temporarily unavailable or unusable

Actions to Be Taken for Each Threat

Mitigating threats refers to the process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures. “A mitigation consists of one or more controls whose purpose is to prevent a successful attack against the software architecture’s confidentiality, integrity, and availability” (Peterson, Hope, & Lavenhar, 2013). In the case of ATM, the actions that can be taken to mitigate threats are to:

- Installing cameras at the ATMs to prevent attackers and to catch any malicious activity
- Install ATMs in well-lit areas
- Fraudulent device inhibitors that prevent scammers from being able to scan cards
- Two-step verification such as asking a personal question that only the user would know
- Fraud detection software that monitors banking systems for unusual purchases
- Encryption of user data such as passwords
- Encryption of hard drives to prevent hackers from gaining access to computers within the ATM
- Increase password complexity such as adding special characters and numbers and not allowing common passwords to be used
- Lock the user out of the system after failed number of attempts and making them have to call support to regain access

After these threats are mitigated, there must be a system in place to manage the risk. “Risk management is the process of continually assessing and addressing risk throughout the life of the software” (Peterson, Hope, & Lavenhar, 2013). It is an ongoing process that uses the analysis, mitigations, metrics, and other processes and tools to manage risk for the organization.

Validating the Model and Threats, and Verification of Success of Actions Taken

There are multiple data validation methods but the one that pertains most to the ATM threat model would be Predictive Validation which “is used to predict (forecast) the system's behavior, and then the system's behavior and the model’s forecast are compared to determine if they are the same. The system's data may come from an operational system or be obtained by conducting experiments on the system, e.g., field tests" (Verification and Validation of Simulation Models, 2018). Using the predictive model can help the bank scope out vulnerabilities before an attacker has a chance to exploit them.

Conclusion

"The overwhelming number of new threats added daily to cyber ecosystems has moved threat modeling from a theoretically interesting concept into a current information security standard" (Security Threat Modeling Methodologies: Comparing Stride, VAST & More, 2019). As the methodologies of threat modeling evolve, businesses recognizing the importance of developing threat models throughout a software development lifecycle.

References

Application Threat Modeling. (n.d.). Retrieved July 18, 2020, from https://owasp.org/www-community/Application_Threat_Modeling

Peterson, G., Hope, P., & Lavenhar, S. (2013, July 02). Architectural Risk Analysis. Retrieved July 21, 2020, from https://us-cert.cisa.gov/bsi/articles/best-practices/architectural-risk-analysis/architectural-risk-analysis

Security Threat Modeling Methodologies: Comparing Stride, VAST & More. (2019, September 03). Retrieved July 18, 2020, from https://threatmodeler.com/threat-modeling-methodologies-overview-for-your-business/

Verification and Validation of Simulation Models. (2018, July 22). Retrieved July 21, 2020, from https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/other-se-lifecycle-building-blocks-articles/verification-and-validation-of-simulation-models