Unit 2 Seminar

Title: Threat Modelling Exercises

Threat Modelling Model for a Large International Bank Based in the UK.

1. **Introduction:**

This threat modelling exercise aims to identify and assess security threats to HSBC Bank's Automatic Teller Machines (ATMs) system. This document provides an overview of the threat modelling process, risks, and recommended mitigations.

According to Synopsys (N.D.), threat modelling entails determining security needs, identifying possible security risks and vulnerabilities, determining the severity of these threats and vulnerabilities, and ranking the best remediation strategies. According to the Bank of England's Financial Stability Report by Terranova Security (N.D.), cyber risks might seriously jeopardise crucial areas of vulnerability such as people, processes, systems and data.

2. **Scope definition:**

The HSBC, a UK-based global bank, was initially called The Hong Kong and Shanghai Banking Corporation and was later known as Hong Kong Bank in some countries (Wikipedia Contributors, 2019). Cybercrime is made possible by HSBC's internet services, which include card transactions, ATMs, online, mobile, and phone banking. TrendMicro (N.D.) reports that staff of big commercial organisations' finance departments are becoming the focus of cybercriminals. They target ATMs, SWIFT networks, payment gateways, card processing systems, and the bank's infrastructure. They also tamper with payment systems.

HSBC Bank offers 24/7 services, including cash withdrawal, payment, money transfer, fund, and foreign exchange transactions (HSBC, N.D.).

This Threat Modelling will focus on HSBC's Automatic Teller Machines (ATMs), revolutionising cash transactions by providing quick and convenient access. ATMs allow customers to withdraw cash, deposit money, transfer funds, and check account balances, among other services. However, customers must be aware of different types of ATM fraud to protect themselves from falling prey to them. Common ATM scams and frauds include skimming, shimming, cloning, trapping, and keyboard jamming (Bajaj Fiserv, N.D.).

Knowing about these scams and being cautious when using ATMs, HSBC can advise customers to prevent them from becoming ATM fraud victims.

3. ATM's Overview

ATMs have two main parts: the cabinet and the safe. The cabinet contains the ATM computer, network equipment, card reader, keyboard (PIN pad), and cash dispenser. The safe has only the cash dispenser and cash acceptance module. The computer runs on Windows in a particular embedded version explicitly designed for ATM use. User-facing applications run in kiosk mode and communicate with ATM peripherals using XFS. An ATM contacts the bank's processing centre to process transactions secured by wired or wireless connections (Positive Technologies, 2018).

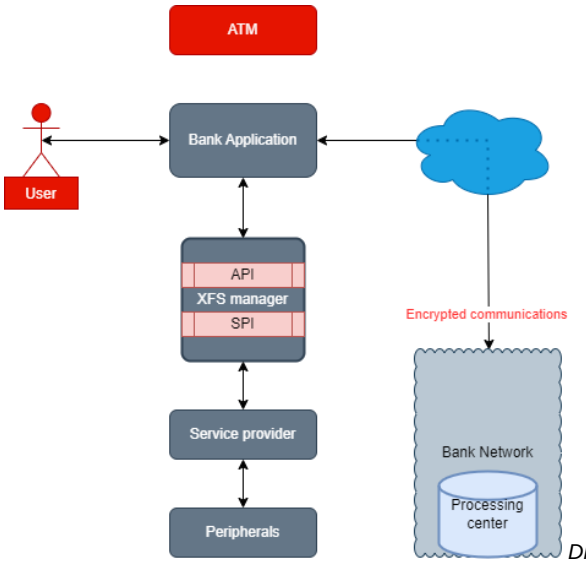


Diagram based on the ideas of Positive Technologies (2018)

4. Types of vulnerabilities

Four categories of ATM security vulnerabilities may be distinguished according to Positive Technologies (2018):

- application control vulnerabilities.
- poor system or device setup.
- inadequate network security.
- and inadequate peripheral security.

With insufficient network security, criminals can exploit network services, intercept communications, and attack equipment. Peripheral security issues frequently result in a need for more authentication between peripherals and the ATM operating system, which gives thieves access to card data and cash. While application control vulnerabilities can arise from system code flaws, improper setup can lead to security breaches (Positive Technologies, 2018).

Logical attacks can be divided into malware-based attacks and black box attacks, as explained by Umawing (2019). Malware-based attacks involve malicious software like Ploutus, Anunak/Carbanak, Cutlet Maker, and SUCEFUL. On the other hand, black box attacks involve manipulating an electronic device without authorisation to issue ATM commands. These attacks are hard to trace because they don't rely on malware.

5. Risk Assessment

5.1. Methodology: Qualitative risk assessment

Risk assessment aims to pinpoint potential risks and their possible impact on decision-making. This can be accomplished through either qualitative or quantitative means. Qualitative assessments generate non-numerical risk estimates, which are often employed when financial or specialised resources are limited. Risk identification, characterisation, and analysis are the two principal functions of qualitative risk assessment (Institute for Water Resources US Army Corps of Engineers, N.D.).

5.2. Assets

The following assets list about the ATMs represents a significant vulnerability that needs to be addressed:

- ATM
- Network Devices
- Data Centre
- Internal Network
- Servers

5.3. Threats:

- denial of service.
- malicious software injection.
- sensitive data disclosure.
- configuration file modification.
- privilege settings modification.
- software component modification.
- test utility exploitation.

5.4. Risks

ATMs are commonly used for financial transactions and are linked to a processing centre via the ATM Active Directory. Banks also have an internal network that manages various services such as SMS, phone, internet banking, and biometric authentication. According to Kochetova et al. (N.D.), there are potential risks that pose a threat to both customers and banks, which include:

- Attacks on hardware components.
- Malware attacks.
- Attacks on the network layer.
- Network attacks on biometric databases.

5.5. Strategies for Mitigation

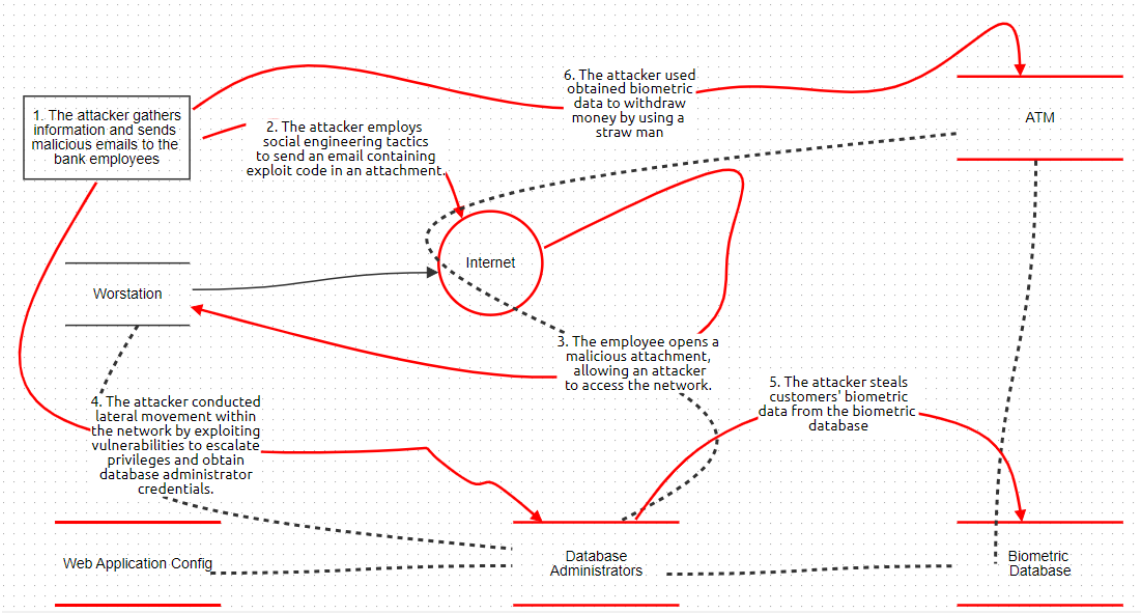
Braeuer et al. (2015) highlight the growing sophistication of logical attacks that well-organized groups frequently execute. These malicious actors employ novel methods and approaches to conduct ATM crimes, which pose significant threats to ATM

networks. Since ATM networks run on the Internet protocol, they are susceptible to the same kind of attacks that affect other IP-related networks. As a result, various measures can be taken to mitigate these risks, including:

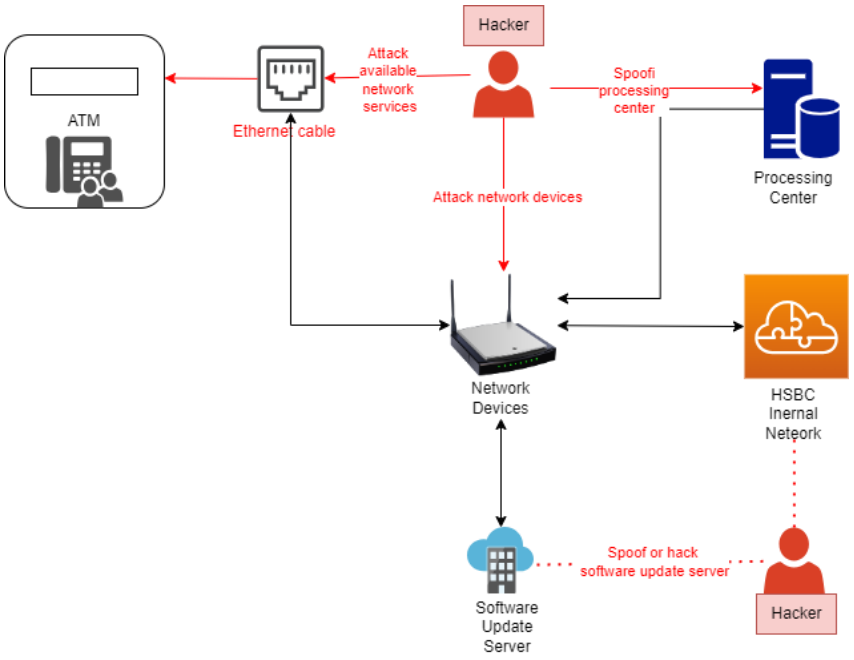
- Implemented logical ATM security systems and allowed listing.
- Physical protection.
- Patch management to ensure timely and efficient protection.

5.6. Data Flow Diagrams

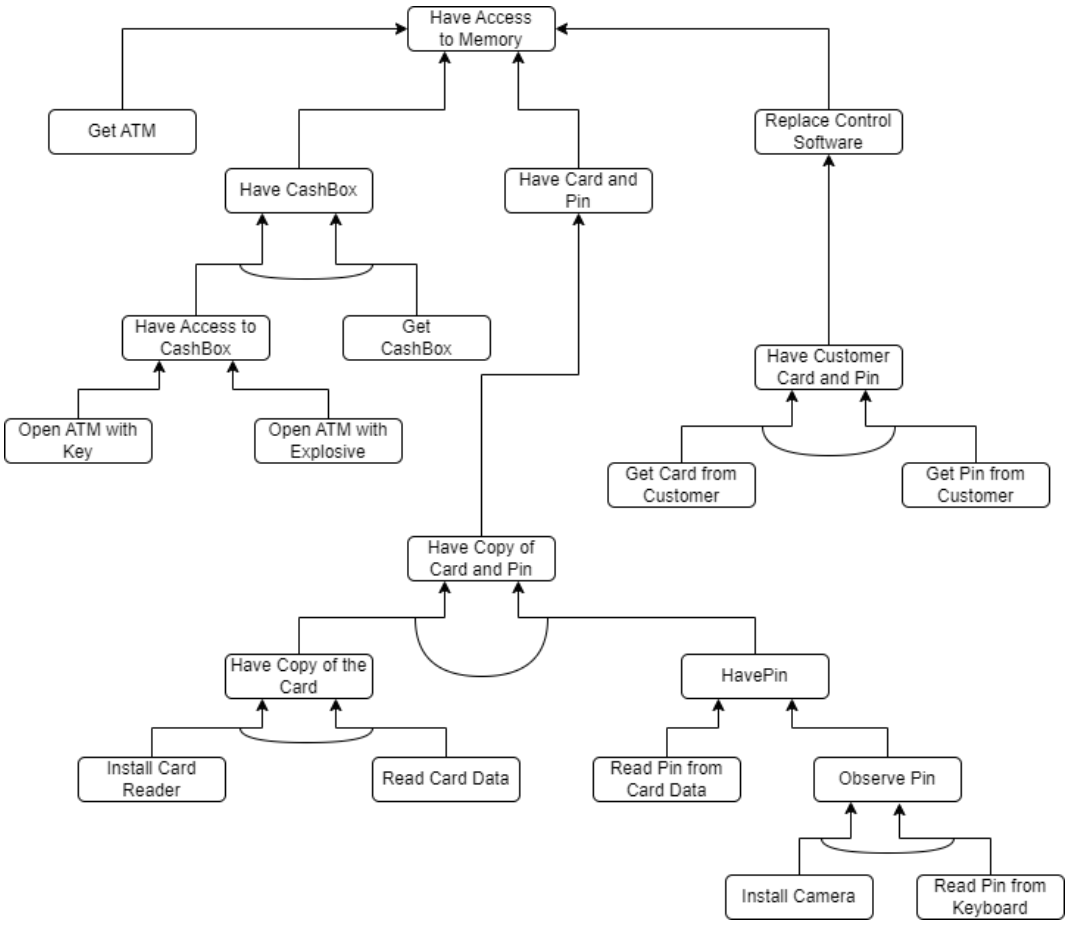
To launch a network-level attack on an ATM, an attacker must gain access to its connected network. This can be done remotely if the attacker works for the bank or internet service provider. If not, the attacker must physically enter the ATM and disconnect the Ethernet wire to either swap out the modem or connect a malicious device. Once done, the attacker can connect with the device, target accessible network services, or attempt man-in-the-middle attacks. Sometimes, the modem may be located outside the ATM cabinet, making it easier for the attacker to tamper with the device without accessing the ATM itself (Positive Technologies, 2018).



"Stealing biometric data from the biometric database" is the attack scenario. Data flow is based on Kochetova et al.'s (N.D.) ideas.



(Positive Technologies, 2018)



An example of an attack against an ATM using an attack tree is by Moeckel (2020).

5.7. STRIDE model

The STRIDE threat model, developed by Microsoft engineers, is a comprehensive guide to identifying potential threats in a system. It is designed to be used with a model of the target system, enabling it to be highly effective in evaluating individual systems (Gonzalez, 2020).

Here is an example of the STRIDE model for the HSBC ATM attack:

Threat situation	Property Violated	What the attackers are capable of
Spoofing	Authentication	Phishing attacks involve spoofing process centres. Attackers can then steal credentials and transfer money (Shostack, 2014).
Tampering	Integrity	Network tampering involves extracting and modifying data before forwarding it to the attacker's machine (Shostack, 2014).
Repudiation	Non-Repudiation	It uses a payment method that belongs to someone else without permission (Shostack, 2014).
Information Disclosure	Confidentiality	Uses error cases to extract machine secrets (Shostack, 2014).
Denial of service	Availability	It makes enough inquiries to cause the system to lag (Shostack, 2014).
Elevation of Privilege	Authorisation	Send data that the code cannot process correctly (Shostack, 2014).

5.8. CVSS

According to a report by The Hacker News (2023), ScrutisWeb's ATM monitoring software has four security flaws related to CVSS. These vulnerabilities enable hackers to access ATMs, upload data, and restart terminals remotely. With one of the vulnerabilities, an attacker can upload and run any file, while the other three allow unauthorised access to files, decryption of passwords, and viewing of profile data. Below are further details about the four security flaws:

- CVE-2023-35189 - Remote code execution vulnerability (CVSS score: 10.0)
- CVE-2023-33871 - Directory traversal vulnerability (CVSS score: 7.5)

- CVE-2023-38257 - Insecure direct object reference vulnerability (CVSS score: 7.5)
- CVE-2023-35763 - Cryptographic vulnerability (CVSS score: 5.5)

6. Recommendations:

In light of the potential risks, it is essential to note that any attacks on HSBC ATMs would have significant repercussions. The resulting losses could significantly impact the bank's reputation, customer relationships, and overall business operations. Furthermore, such attacks could also lead to a breach of GDPR laws, resulting in legal and financial consequences for the bank. Therefore, HSBC must take all necessary measures to safeguard its ATMs against potential threats and ensure its customer data is always protected (Deloitte, 2019).

References:

- Synopsys (N.D.). *What Is Threat Modeling and How Does It Work?* | *Synopsys*. [online] www.synopsys.com. Available at: https://www.synopsys.com/glossary/what-is-threat-modeling.html.
- Terranova Security (N.D.). *Cyber Attacks Pose the Biggest Risk to UK Banks* | *Terranova Security*. [online] Available at: https://terranovasecurity.com/blog/cyber-attacks-bank-of-england/.
- Wikipedia Contributors (2019). *HSBC*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/HSBC.
- TrendMicro (N.D.). *Banks Under Attack: Tactics and Techniques Used to Target Financial Organizations - Security News*. [online] Available at: https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/banks-under-attack-tactics-and-techniques-used-to-target-financial-organizations.
- HSBC (N.D.). *About Our ATMs* | *Features and Advantages* | *ATM Banking* | *HSBC*. [online] Available at: https://www.hsbc.com.tr/en/direct-banking/atm-banking/about-our-atms [Accessed 11 Feb. 2024].
- Bajaj Fiserv (N.D.). *Everything about ATM Frauds, its Types and Prevention Methods* | *Bajaj Finance Insurance Mall*. [online] Available at: https://www.bajajfinserv.in/insurance/secure-yourself-from-atm-fraud.
- Positive Technologies (2018). *ATM logic attacks: scenarios, 2018*. [online] Ptsecurity.com. Available at: https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/.
- Umawing, J. (2019). *Everything you need to know about ATM attacks and fraud: part 2* | *Malwarebytes Labs*. [online] Malwarebytes. Available at: https://www.malwarebytes.com/blog/news/2019/08/atm-attacks-and-fraud-part-2.
- Institute for Water Resources US Army Corps of Engineers (N.D.). *Corps Risk Analysis Gateway Training Module Risk Assessment - Qualitative Methods.* Available at: https://www.iwr.usace.army.mil/Portals/70/docs/risk/Risk_Assessment_Qualitative_Methods_dft.pdf?ver=2018-07-03-134517-720.
- Kochetova, O., Osipov, A. & Novikova, Y. (N.D.). *FUTURE ATTACK SCENARIOS AGAINST AUTHENTICATION SYSTEMS, COMMUNICATING WITH ATMS 2*. Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/02/20114930/Future_ATM_attacks_report_eng.pdf.
- Braeuer, J., Gmeiner, B. & Sametinger, J. (2015). *ATM Security A Case Study of a Logical Risk Assessment*. [online] Available at: https://se.jku.at/wp-content/uploads/2016/04/2015.ATM-security.pdf [Accessed 12 Feb. 2024].
- Gonzalez, C. (2020). *6 Threat Modeling Methodologies: Prioritize & Mitigate Threats*. [online] Exabeam. Available at: https://www.exabeam.com/information-security/threat-modeling/.
- Shostack, A. (2014). *Threat Modeling: Design for Security 1st ed*. John Wiley & Sons, Incorporated.

- The Hacker News (2023). *Multiple Flaws Found in ScrutisWeb Software Exposes ATMs to Remote Hacking*. [online] Available at: https://thehackernews.com/2023/08/multiple-flaws-found-in-scrutisweb.html [Accessed 12 Feb. 2024].
- Deloitte (2019). *How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on.* Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf [Accessed 19 Feb. 2024].