In-Class Exercise: Abuse/Misuse Cases- Group 9

BY:

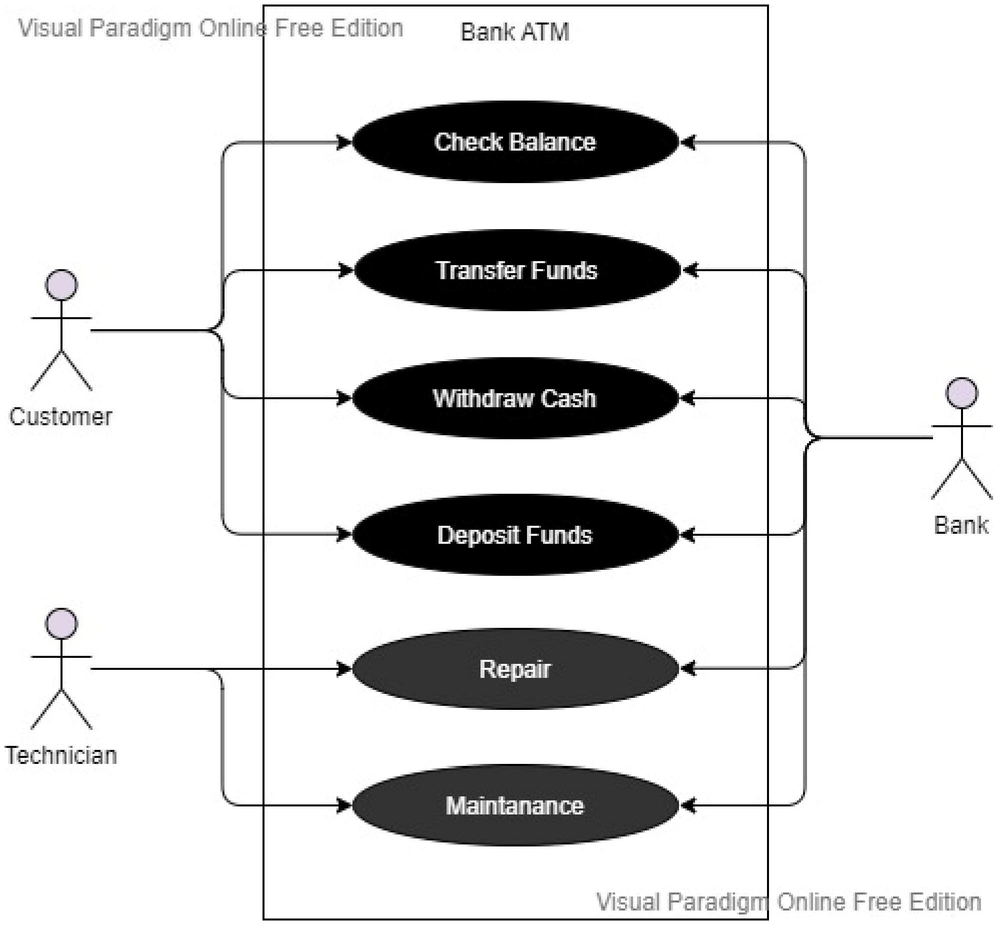
Atishay Jain

Meet Rajeshkumar Jain

Vishwesh Malur Somashekar

Amith Vishnu

Saurabh Agrawal



The primary functions of the ATM in this diagram are:

1.Check account balance

2.Withdraw cash

3.Deposit cash

4.Transfer funds

The abuse/misuse cases in this diagram are:

1.

Actors – Attacker
• Description – **Card skimming**
• Data (assets) – User information
• Attacks – In this case, an attacker attaches a device to the card reader on the ATM that captures the user's card information and PIN. This information can then be used to make fraudulent transactions.
• Mitigations – Encryption of sensitive data, such as card information and PINs, to protect it from unauthorized access.

• Requirements – tamper-detection system that alerts the bank if any unauthorized modifications are made to the ATM.

2.

Actors – Attacker(s)
• Description – **Transaction reversal fraud**
• Data (assets) – Bank Funds
• Attacks –.: In this case, an attacker makes a withdrawal from the ATM and then reverses the transaction by claiming that it was unauthorized. The funds are then returned to the attacker's account
• Mitigations – Transaction validation systems that check the validity of each transaction and require the user to provide additional authentication before a reversal can be performed. This can help prevent attackers from reversing legitimate transactions to steal funds.

Authentication protocols that require multiple forms of authentication, such as a combination of a user's card, PIN, and biometric information, to access the ATM. This can help prevent unauthorized access to the ATM and the theft of sensitive information.

• Requirements – transaction validation system that checks the validity of each transaction and requires the user to provide additional authentication before a reversal can be performed.

3.

Actors – Attacker(s)
• Description – **Malware injection**:
• Data (assets) – What is threatened by the misuse
• Attacks – In this case, an attacker infects the ATM with malware that captures user information and PINs and sends them to the attacker.
• Mitigations – Regular security updates and antivirus scanning to detect and remove malware that could be used to capture card information and PINs.

A firewall on the ATM to prevent unauthorized access to the ATM's network and to block potential malware infections.
• Requirements –regular security updates and antivirus scanning to detect and remove malware.

4.

Actors – Attacker(s)
• Description – **Physical theft**
• Data (assets) – Cash
• Attacks – In this case, an attacker physically steals the cash from the ATM
• Mitigations – Surveillance systems that monitor the ATM and alert the bank if any suspicious activity is detected. These systems can help identify attempts to break into the ATM or physically steal cash from it.

Tamper-detection systems that alert the bank if any unauthorized modifications are made to the ATM. These systems can help identify attempts to attach skimming devices or other devices that could be used to commit physical theft attacks.

• Requirements – surveillance system that monitors the ATM and alerts the bank if any suspicious activity is detected.