Threat Modeling for an Online Banking System

Assets

- Customer data (personal information, financial data, transaction history)
- Financial transactions
- Banking infrastructure (servers, networks, databases)
- Reputation and customer trust

Threats

- Unauthorized access
- Data breaches
- Denial of Service (DoS) attacks
- Man-in-the-middle (MitM) attacks
- Phishing attacks
- Malware infections
- Insider threats
- Social engineering attacks

Vulnerabilities

- Weak password policies
- Insecure data transmission
- Vulnerable software and systems
- Insufficient access controls
- Lack of employee training
- Poor physical security
- Inadequate network security

Attacks

- Brute force attacks
- Password guessing
- SQL injection
- Cross-site scripting (XSS)
- Man-in-the-middle attacks

- Phishing
- Malware infection
- Denial of Service (DoS)
- Insider fraud
- Social engineering

Risks

- Financial loss for customers and the bank
- Reputation damage
- Legal liabilities
- Loss of customer trust
- Data privacy breaches
- Business interruption

Exploits

- Account takeover
- Funds transfer
- Data exfiltration
- System disruption
- Identity theft
- Fraudulent transactions

Impacts

- Financial loss
- Reputation damage
- Legal penalties
- Loss of customers
- System downtime
- Compliance violations

Example Threat Scenario:

- Threat: Unauthorized access
- Vulnerability: Weak password policy
- Attack: Brute force attack
- Risk: Account takeover, financial loss
- Exploit: Funds transfer to attacker's account
- Impact: Financial loss for the customer and the bank, damage to reputation

Mitigation Strategies

- Strong password policies
- Encryption
- Firewalls
- Intrusion detection systems
- Regular security audits
- Employee training
- Incident response plan
- Multi-factor authentication
- Fraud detection systems