Threat Modeling

- Threat Modeling is a systematic process used to identify, assess and prioritize potential security threats to a system application or network.
- The goal of threat modeling is to understand the security risks that a system may face and to develop strategies to mitigate those risks before they can be exploited by attacks.

ONLINE BANKING SYSTEM

Let us explore banking applications using the STRIDE framework, which focuses on identifying potential threats related to Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

1. Assets

- **Customer Data**: Personal and financial information, including names, addresses, Social Security Numbers (SSNs), account numbers, etc.
- **Bank Account Information**: Details of savings, checking, credit accounts, transaction histories, and balances.
- **Authentication Data**: Usernames, passwords, multi-factor authentication (MFA) tokens, security questions, etc.
- **Transaction Data**: Records of financial transactions, fund transfers, bill payments, etc.
- **Banking Application Servers**: The servers hosting the banking application, including web servers, databases, and APIs.
- **Internal Network**: The internal infrastructure that supports the banking operations.

2. Potential Threats

- **Spoofing**: An attacker pretends to be a legitimate user (e.g., using stolen credentials) to gain unauthorized access.
- **Tampering**: An attacker alters data in transit or stored on the servers (e.g., modifying account balances).
- **Repudiation**: A user denies performing an action, and the system lacks sufficient logging to prove otherwise (e.g., denying an unauthorized fund transfer).
- **Information Disclosure**: Unauthorized access to sensitive customer or financial information (e.g., data breach exposing customer SSNs).
- **Denial of Service (DoS)**: Attacks that make the banking service unavailable to legitimate users (e.g., overwhelming the server with traffic).
- **Elevation of Privilege**: A user gains higher access levels than permitted (e.g., a user escalating privileges to perform administrative functions).

3. Vulnerabilities

- **Weak Password Policies**: Allowing weak or easily guessable passwords.
- **Insufficient Encryption**: Data, either in transit or at rest, is not properly encrypted.
- **Lack of Multi-Factor Authentication (MFA)**: Relying solely on passwords without additional authentication layers.
- **Poorly Configured Firewalls/Intrusion Detection Systems (IDS)**: Ineffective protection against unauthorized access or attacks.
- **Insufficient Input Validation**: Failing to validate input can lead to SQL injection or other injection attacks.
- **Outdated Software**: Running outdated software versions that contain known vulnerabilities.

4. Potential Attacks

- **Phishing Attacks**: Trick users into providing credentials that attackers can use for spoofing.
- **Man-in-the-Middle (MitM) Attacks**: Intercepting and altering communications between the user and the bank's servers.
- **SQL Injection**: Injecting malicious SQL code to manipulate the database.
- **Distributed Denial of Service (DDoS)**: Overwhelming the banking system with traffic to cause a service outage.
- **Brute Force Attacks**: Attempting to guess passwords by systematically trying many possibilities.
- **Privilege Escalation**: Exploiting vulnerabilities to gain unauthorized administrative access.

5. Risks

- **Financial Loss**: Direct financial loss to customers or the bank due to fraudulent transactions.
- **Reputation Damage**: Loss of customer trust due to breaches or service outages.
- **Regulatory Fines**: Penalties for failing to comply with data protection regulations (e.g., GDPR, CCPA).
- **Legal Consequences**: Lawsuits from customers or partners due to security breaches.
- **Operational Disruption**: Downtime or degraded performance impacting banking operations.

6. Exploits

- **Exploiting Unpatched Software**: Attacking vulnerabilities in outdated systems.
- **Credential Stuffing**: Using stolen or leaked credentials to gain unauthorized access.

- **Session Hijacking**: Taking over a user’s session by stealing session cookies.
- **Cross-Site Scripting (XSS)**: Injecting malicious scripts into web pages viewed by users.
- **Ransomware**: Encrypting the bank’s data and demanding payment for decryption.

7. Impact

- **Data Breach**: Loss or exposure of sensitive customer data leading to identity theft.
- **Financial Fraud**: Unauthorized transactions resulting in significant financial losses.
- **System Downtime**: Disruption of banking services leading to customer dissatisfaction and financial impact.
- **Regulatory Action**: Fines and legal actions resulting from non-compliance with regulations.
- **Customer Trust Erosion**: Long-term damage to the bank’s reputation, potentially leading to loss of customers.

8. Mitigation Strategies

- **Strong Authentication**: Implement multi-factor authentication (MFA) and enforce strong password policies.
- **Encryption**: Ensure data is encrypted both in transit and at rest.
- **Regular Security Audits**: Conduct frequent security assessments and penetration testing.
- **Patch Management**: Regularly update and patch systems to address known vulnerabilities.
- **Monitoring and Logging**: Implement robust logging and monitoring to detect and respond to suspicious activities quickly.
- **Network Security**: Configure firewalls, intrusion detection systems, and anti-DDoS solutions to protect the infrastructure.