Unit 4 Seminar: Threat Modelling Exercises

Scenario: A Large International Bank Based in the UK

Introduction

Threat modelling is a systematic approach to identifying, analysing, and mitigating potential security risks. For this exercise, the focus is on a large international bank in the UK, a critical infrastructure organisation requiring robust protections due to its exposure to cyberattacks, fraud, and insider threats. The STRIDE, DREAD, Attack Trees, and ATT&CK libraries will be used, along with insights from the Threat Modelling Manifesto (2020), OWASP Threat Modelling Cookbook (2021), and Common Vulnerability Scoring System (CVSS) critiques.

Threat Modelling Approach:

This exercise will utilise a combination of methodologies, drawing from Shostack (2018), Spring et al. (2021), the Threat Modelling Manifesto, the OWASP Threat Modelling Cookbook, and the ATT&CK framework.

1. Approach to Threat Modelling

STRIDE Framework

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges) is used to analyse threats in each system component (Shostack, 2018):

1. **Spoofing:** Unauthorised access to customer accounts through phishing or credential stuffing.
2. **Tampering:** Manipulation of transaction data in the core banking systems.
3. **Repudiation:** Lack of audit trails for administrative actions in banking systems.
4. **Information Disclosure:** Breaches leading to exposure of sensitive financial information.
5. **Denial of Service (DoS):** Attacks on online banking platforms disrupting services.
6. **Elevation of Privileges:** Exploitation of internal system vulnerabilities by attackers or malicious insiders.

DREAD Model

The DREAD model evaluates and prioritises threats based on their:

1. **Damage potential:** Impact of fraudulent transactions or customer data breaches.
2. **Reproducibility:** Ease of replicating attack vectors, such as SQL injection or phishing.
3. **Exploitability:** Vulnerabilities in outdated software or weak configurations.
4. **Affected users:** The large number of customers relying on online banking platforms.
5. **Discoverability:** The likelihood of attackers discovering vulnerabilities through automated tools or reconnaissance.

Attack Trees

Attack trees are used to visualise potential attack paths, starting with the root goal and branching into sub-objectives:

- **Goal:** Compromise customer financial accounts.
    - Sub-goals:
        - Gain access to customer credentials.
            - Methods: Phishing, brute force, or social engineering.
        - Exploit vulnerabilities in online banking APIs.
            - Methods: Injection attacks or session hijacking.

2. Threat Libraries and OWASP Integration

ATT&CK Libraries

The MITRE ATT&CK framework informs the model by identifying tactics, techniques, and procedures (TTPs) used by threat actors. Relevant techniques include:

- **Credential Dumping (T1003):** Extracting credentials from memory.
- **Data Exfiltration (T1041):** Transferring sensitive data outside the organization.

- **Privilege Escalation (T1068):** Exploiting vulnerabilities to gain higher permissions.

OWASP Threat Modelling Cookbook

The OWASP Threat Modelling Cookbook (2021) provides a practical guide for implementing the STRIDE framework. It highlights the importance of continuously validating the model with stakeholders and integrating mitigations into the software development lifecycle (SDLC).

3. Critiques and Improvements Using CVSS Insights

Spring et al. (2021) discuss limitations of the CVSS, particularly its inability to capture complex, multi-stage attacks. This critique reinforces the need for a more contextualised risk scoring approach, such as:

- Combining STRIDE and DREAD for a comprehensive analysis.
- Integrating real-world attack scenarios using ATT&CK techniques.
- Considering business impact metrics alongside technical severity.

Key Assets and Threats:

- **Customer Data:**
    - **Threats:**
        - **Information Disclosure:** Credential theft through phishing. Data breaches (e.g., phishing, social engineering, malware) leading to the exposure of sensitive customer information (financial details, personal data).
        - **Tampering:** Unauthorised modification or deletion of customer data, potentially impacting financial transactions or personal records.
        - **Spoofing:** Identity theft and fraudulent transactions using stolen credentials.
    - **Mitigation:**
        - Strong authentication mechanisms (multi-factor authentication, biometrics).
        - Data encryption both in transit and at rest.

        - Regular security awareness training for employees and customers.
        - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

- **Financial Transactions:**
    - **Threats:**
        - **Denial of Service:** Distributed Denial of Service (DDoS) attacks disrupting online banking services, impacting customer access and financial operations.
        - **Tampering:** Manipulation of financial transactions, including unauthorised transfers or fraudulent payments.
        - **Repudiation:** Disputed transactions due to unauthorised access or system vulnerabilities.
    - **Mitigation:**
        - Fraud detection systems based on machine learning and behavioural analysis.
        - Secure transaction processing protocols (e.g., SSL/TLS).
        - Regular system monitoring and vulnerability assessments.
- **System Integrity:**
    - **Threats:**
        - **Elevation of Privilege:** Attacks exploiting system vulnerabilities to gain unauthorised access to critical systems and data.
        - **Denial of Service:** Attacks targeting critical infrastructure, disrupting core banking operations.
        - **Tampering:** Malicious software infiltrating systems and compromising system integrity.
    - **Mitigation:**
        - Regular security patches and updates.
        - Secure system configurations and access controls.

        - Network segmentation and isolation of critical systems.

Threat Modelling Process:

1. **Define Scope:** Clearly define the scope of the threat model, focusing on the online banking platform and its key components (e.g., customer portal, mobile app, backend systems).
2. **Identify Assets:** Determine the critical assets within the defined scope, including customer data, financial transactions, and system infrastructure.
3. **Threat Identification:** Utilise STRIDE to systematically identify potential threats across each category.
4. **Threat Analysis:** Employ DREAD and CVSS to score and prioritise identified threats based on their severity and potential impact.
5. **Attack Tree Analysis:** Develop attack trees to visualise potential attack paths and identify vulnerabilities at different levels of the system.
6. **Mitigation Strategies:** Develop and implement appropriate mitigation strategies based on identified threats and vulnerabilities.
7. **Continuous Monitoring and Review:** Regularly review and update the threat model to reflect changes in the threat landscape, system architecture, and business requirements.

Mitigation Strategies and Recommendations

- **Regular Penetration Testing:** Identify and address vulnerabilities proactively.
- **Zero-Trust Architecture:** Limit implicit trust and enforce continuous verification.
- **Employee Training:** Reduce phishing risks through awareness campaigns.
- **Incident Response Planning:** Prepare for swift mitigation of successful attacks.

Tools and Technologies:

- **OWASP Threat Dragon:** A popular open-source tool for visual threat modelling.
- **MITRE ATT&CK Navigator:** A knowledge base and interactive visualisation tool for cyber adversary emulation.

- **Security Information and Event Management (SIEM) systems:** For centralised log management and threat detection.

Conclusion:

By employing a comprehensive threat modelling approach, incorporating insights from Shostack (2018), Spring et al. (2021), the Threat Modelling Manifesto, the OWASP Threat Modelling Cookbook, and the ATT&CK framework, organisations can proactively identify and mitigate cyber threats to their online banking platforms, ensuring the security and resilience of their critical systems and protecting customer data and financial assets.

References:

- Shostack, A. (2018). Threat Modelling: Designing for Security. Addison-Wesley Professional.
- Spring, N., et al. (2021). The Common Vulnerability Scoring System: A Critical Review. arXiv preprint arXiv:2102.06446.
- The Threat Modelling Manifesto. [Online] Available at: https://www.securitycompass.com/resource_videos/a-new-approach-to-threat-modeling/
- OWASP Threat Modelling Cookbook. [Online] Available at: https://github.com/OWASP/threat-model-cookbook
- MITRE ATT&CK. [Online] Available at: https://attack.mitre.org/
- IEEE Standards Association. (2014). IEEE Std 15288-2008, Systems and Software Engineering - System Safety Engineering.