Threat Modeling using(todo)

Threat modeling is a structured approach to identifying and assessing potential security threats and vulnerabilities in a system. It helps organizations understand and mitigate risks by systematically analyzing their systems and identifying potential attack vectors. There are several frameworks and methodologies for threat modeling, each with its approach and focus. Here are some of the most widely used frameworks:

1. STRIDE

Overview: STRIDE is a threat modeling framework developed by Microsoft that categorizes threats based on different types of attacks. It is useful for identifying potential security threats during the design phase of a system.

Categories:

- **Spoofing:** Impersonating someone or something.
- **Tampering:** Altering data or code.
- **Repudiation:** Denying an action or transaction.
- **Information Disclosure:** Exposing confidential information.
- **Denial of Service (DoS):** Disrupting service availability.
- **Elevation of Privilege:** Gaining unauthorized access or privileges.

Usage:

1. Identify and document all system components and their interactions.
2. Analyze each component for threats in each STRIDE category.
3. Develop mitigations for identified threats.

Resources:

- Microsoft STRIDE Overview

2. DREAD

Overview: DREAD is a risk assessment model used to evaluate the severity of threats identified through threat modeling. It helps prioritize which threats to address based on their impact and likelihood.

Categories:

- **Damage:** The impact of the threat if it were to exploit a vulnerability.
- **Reproducibility:** How easily the attack can be reproduced.
- **Exploitability:** The ease with which an attacker can exploit the vulnerability.
- **Affected Users:** The number of users affected by the threat.
- **Discoverability:** How easy it is to discover the vulnerability.

Usage:

1. Assign a score (typically 1-10) for each DREAD category for each threat.
2. Calculate an overall risk score by aggregating the scores.
3. Prioritize threats based on their risk scores and address the most severe ones first.

Resources:

- DREAD Risk Assessment Model

3. PASTA (Process for Attack Simulation and Threat Analysis)

Overview: PASTA is a risk-centric threat modeling methodology designed to simulate attacks and analyze potential threats from an attacker's perspective. It is a more dynamic approach compared to other frameworks.

Phases:

1. **Definition of Objectives:** Define security objectives and scope.
2. **Definition of the Technical Scope:** Document system architecture and components.
3. **Application Decomposition:** Break down the application into functional components.
4. **Threat Analysis:** Identify and analyze potential threats and vulnerabilities.
5. **Attack Simulation:** Simulate attacks to assess the impact and feasibility.
6. **Risk and Impact Analysis:** Evaluate the impact and likelihood of threats.
7. **Mitigation and Remediation:** Develop and implement mitigation strategies.

Resources:

- PASTA Overview

4. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Overview: OCTAVE is a risk-based threat modeling methodology focused on organizational and operational aspects. It is used to evaluate security risks by identifying critical assets, vulnerabilities, and potential threats.

Phases:

1. **Identify Critical Assets:** Determine and document valuable assets.
2. **Identify Threats and Vulnerabilities:** Analyze potential threats and vulnerabilities affecting critical assets.
3. **Evaluate Risks:** Assess the risks associated with each threat and vulnerability.
4. **Develop Mitigation Strategies:** Formulate and implement strategies to mitigate identified risks.

Resources:

- OCTAVE Overview

5. Attack Trees

Overview: Attack Trees provide a graphical representation of how an attacker might achieve their goals by exploiting vulnerabilities. They help visualize potential attack scenarios and their associated risks.

Usage:

1. **Define Attack Goals:** Identify the goals or objectives an attacker might aim to achieve.
2. **Develop Attack Trees:** Create a tree structure showing various attack paths and methods.
3. **Analyze and Prioritize:** Evaluate and prioritize attack paths based on their feasibility and impact.
4. **Develop Mitigation Strategies:** Implement security measures to address the most critical attack paths.

Resources:

- Attack Trees Overview

6. Harmonia

Overview: Harmonia is a threat modeling framework that emphasizes integration with the software development lifecycle and focuses on integrating threat modeling into existing processes.

Phases:

1. **Identify Assets:** Determine valuable assets and their importance.
2. **Identify Threats:** Analyze potential threats and their impact on assets.
3. **Assess Vulnerabilities:** Identify and assess vulnerabilities that could be exploited by threats.
4. **Define Countermeasures:** Develop and implement countermeasures to mitigate identified threats.

Resources:

- Harmonia Framework

7. LINDDUN

Overview: LINDDUN is a privacy-focused threat modeling framework that helps in identifying privacy-related threats in systems and applications.

Categories:

- **Linkability:** Identifying whether different activities or data can be linked to an individual.
- **Identifiability:** Determining if individuals can be identified.
- **Non-repudiation:** Ensuring that actions or transactions cannot be denied.
- **Detectability:** Assessing if the presence of an individual’s data can be detected.
- **Disclosure of Information:** Identifying the potential for unauthorized data disclosure.

- **Unawareness:** Assessing if individuals are unaware of data collection or processing.

Usage:

1. Identify privacy concerns in the system.
2. Analyze the system for threats in each LINDDUN category.
3. Develop privacy-enhancing measures to mitigate identified threats.

Resources:

- LINDDUN Overview

8. MITRE ATT&CK

Overview: MITRE ATT&CK is a knowledge base of adversary tactics and techniques based on real-world observations. It provides a comprehensive framework for understanding and analyzing attack methods.

Categories:

- **Initial Access:** Methods used by attackers to gain entry into a network.
- **Execution:** Techniques used to execute malicious code.
- **Persistence:** Methods to maintain access to compromised systems.
- **Privilege Escalation:** Techniques for increasing access levels.
- **Defense Evasion:** Methods for avoiding detection and evasion.
- **Credential Access:** Techniques for obtaining credentials.
- **Discovery:** Methods for gathering information about the environment.
- **Lateral Movement:** Techniques for moving within the network.
- **Collection:** Methods for gathering data from compromised systems.
- **Exfiltration:** Techniques for transferring data out of the network.
- **Impact:** Techniques for disrupting or damaging systems.

Resources:

- MITRE ATT&CK Overview

9. NIST Cybersecurity Framework (CSF)

Overview: The NIST Cybersecurity Framework is a set of guidelines and best practices for managing cybersecurity risks. While not specifically a threat modeling framework, it provides a comprehensive approach to managing cybersecurity, including threat identification.

Core Functions:

1. **Identify:** Develop an understanding of the organization’s environment and risks.
2. **Protect:** Implement safeguards to ensure the delivery of critical infrastructure services.
3. **Detect:** Implement activities to identify the occurrence of a cybersecurity event.
4. **Respond:** Develop and implement appropriate activities to respond to a detected cybersecurity event.

5. **Recover:** Develop and implement appropriate activities to restore any capabilities or services that were impaired.

Resources:

- NIST Cybersecurity Framework Overview

10. Risk Management Framework (RMF)

Overview: The Risk Management Framework (RMF) provides a structured approach to managing risks by integrating security and risk management activities into the system development lifecycle.

Phases:

1. **Categorize:** Categorize the information system and its environment.
2. **Select:** Select appropriate security controls.
3. **Implement:** Implement the selected security controls.
4. **Assess:** Assess the effectiveness of the implemented controls.
5. **Authorize:** Obtain authorization to operate the system.
6. **Monitor:** Continuously monitor the system and its controls.

Resources:

- Risk Management Framework Overview