**AMRUTHESH**

**241059041**

**CRYPTOLOGY**

**M.E – CYBER SECURITY**

**Frameworks for Threat Modelling**

Threat modeling is a structured process to identify, evaluate, and address potential security threats within a system. It helps in understanding how adversaries could attack the system and provides methods to mitigate those threats.

1. **STRIDE Model**

STRIDE is a widely used framework that categorizes threats into six types:

* **Spoofing**: Impersonating someone else, usually to bypass authentication.
* **Tampering**: Modifying data or code.
* **Repudiation**: Denying that an action occurred, even if it did.
* **Information Disclosure**: Leaking sensitive data.
* **Denial of Service (DoS)**: Preventing legitimate use of services.
* **Elevation of Privilege**: Gaining permissions beyond those originally granted.

**Use case**: STRIDE is primarily used to identify specific types of threats in systems during the design phase.

1. **DREAD Model**

DREAD focuses on the risk assessment of identified threats. The five elements of DREAD are:

* **Damage potential**: How severe the impact will be if the threat is realized.
* **Reproducibility**: How easily the threat can be reproduced.
* **Exploitability**: The difficulty level of exploiting the threat.
* **Affected users**: The number of users impacted by the threat.
* **Discoverability**: How easy it is to discover the threat.

**Use case**: DREAD helps prioritize threats by assigning risk scores, which makes it useful for risk management and decision-making.

1. **PASTA (Process for Attack Simulation and Threat Analysis)**

PASTA is a risk-centric approach focusing on the attack surface and simulating attacks:

* **Stage 1**: Define objectives.
* **Stage 2**: Define the technical scope.
* **Stage 3**: Application decomposition and enumeration of the attack surface.
* **Stage 4**: Threat analysis.
* **Stage 5**: Vulnerability analysis.
* **Stage 6**: Attack modeling and simulation.
* **Stage 7**: Risk and impact analysis.

**Use case**: PASTA is suitable for complex systems where understanding risk from an attacker's perspective is critical.

1. **LINDDUN**

LINDDUN is a privacy threat modeling framework designed to address privacy concerns within a system. It identifies privacy threats based on the following:

* **Link-ability**
* **Identifiability**
* **Non-repudiation**
* **Detectability**
* **Disclosure of information**
* **Unawareness**
* **Non-compliance**

**Use case**: This is used when privacy concerns are a key aspect of the system being designed or reviewed.

1. **Attack Trees**

Attack trees model threats in a hierarchical tree structure where the root node is the goal (e.g., "steal sensitive data") and the leaves represent the various means by which that goal could be achieved. This framework is flexible and can be applied to any type of system.

**Use case**: Attack trees are useful for visualizing the paths an attacker could take to compromise a system.

1. **VAST (Visual, Agile, and Simple Threat modeling)**

VAST provides scalability by aligning with Agile methodologies. It has two parts:

* **Application Threat Modeling**: Focuses on threats to the application and the security requirements.
* **Operational Threat Modeling**: Focuses on the infrastructure, network, and deployments.

**Use case**: VAST is great for modern software development cycles, particularly in organizations that use Agile and DevOps methodologies.

**Steps to Conduct Threat Modeling:**

1. **Identify Assets**: Determine which components or data need protection.
2. **Create an Architecture Diagram**: Visualize the system components, data flow, and interactions.
3. **Identify Threats**: Use frameworks like STRIDE or LINDDUN to identify potential threats.
4. **Assess Threats**: Quantify and prioritize the identified threats using models like DREAD.
5. **Mitigation Planning**: Develop strategies to mitigate or eliminate the identified threats.
6. **Validation**: Continuously validate and refine the model as the system evolves.