What is Threat Modeling?

Threat modeling is a method of optimizing network security by **locating vulnerabilities, identifying objectives**, and **developing countermeasures** to either prevent or mitigate the effects of cyber-attacks against the system.

The Threat Modeling Process

- Threat modeling consists of defining an **enterprise's assets**, **identifying what function each application serves in the grand scheme**, and assembling a **security profile** for each application.
- The process continues with **identifying and prioritizing potential threats**, then **documenting** both the harmful events and what actions to take to resolve them.

Threat Modeling Methodologies

1. STRIDE

A methodology developed by Microsoft for threat modelling, it offers a mnemonic for identifying security threats in six categories:

- **Spoofing**: An intruder posing as another user, component, or other system feature that contains an identity in the modelled system.
- **Tampering**: The altering of data within a system to achieve a malicious goal.
- **Repudiation**: The ability of an intruder to deny that they performed some malicious activity, due to the absence of enough proof.
- **Information Disclosure**: Exposing protected data to a user that isn't authorized to see it.
- **Denial of Service**: An adversary uses illegitimate means to exhaust services needed to provide service to users.
- **Elevation of Privilege**: Allowing an intruder to execute commands and functions that they aren't allowed to.

2. DREAD

Proposed for threat modeling, but Microsoft dropped it in 2008 due to inconsistent ratings. OpenStack and many other organizations currently use DREAD. It's essentially a way to rank and assess security risks in five categories:

- **Damage Potential**: Ranks the extent of damage resulting from an exploited weakness.
- **Reproducibility**: Ranks the ease of reproducing an attack
- **Exploitability**: Assigns a numerical rating to the effort needed to launch the attack.

- **Affected Users**: A value representing how many users get impacted if an exploit becomes widely available.
- **Discoverability**: Measures how easy it is to discover the threat.

3. P.A.S.T.A

This stands for Process for Attack Simulation and Threat Analysis, a seven-step, risk-centric methodology. It offers a dynamic threat identification, enumeration, and scoring process. Once experts create a detailed analysis of identified threats, developers can develop an asset-centric mitigation strategy by analyzing the application through an attacker-centric view.

4. Trike

Trike focuses on using threat models as a risk management tool. Threat models, based on requirement models, establish the stakeholder-defined "acceptable" level of risk assigned to each asset class. Requirements model analysis yields a threat model where threats are identified and given risk values. The completed threat model is then used to build a risk model, factoring in actions, assets, roles, and calculated risk exposure

5. VAST

- Standing for Visual, Agile, and Simple Threat modeling, it provides actionable outputs for the specific needs of various stakeholders such as application architects and developers, cybersecurity personnel, etc.
- VAST offers a unique application and infrastructure visualization plan so that the creation and use of threat models don't require any specialized expertise in security subject matters.

6. Attack Tree

The tree is a conceptual diagram showing how an asset, or target, could be attacked, consisting of a root node, with leaves and children nodes added in. Child nodes are conditions that must be met to make the direct parent node true. Each node is satisfied only by its direct child nodes. It also has "AND" and "OR" options, which represent alternative steps taken to achieve these goals.

7. Common Vulnerability Scoring System (CVSS)

This method provides a way to capture a vulnerability's principal characteristics and assigning a numerical score (ranging from 0-10, with 10 being the worst) showing its severity. The score is then translated into a qualitative representation (e.g., Low, Medium, High, and Critical). This representation helps organizations effectively assess and prioritize their unique vulnerability management processes.

8. T-MAP

T-MAP is an approach commonly used in Commercial Off the Shelf (COTS) systems to calculate attack path weights. The model incorporates UML class diagrams, including access class, vulnerability, target assets, and affected value.

9. OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) process is a risk-based strategic assessment and planning method. OCTAVE focuses on assessing organizational risks only and does not address technological risks. OCTAVE has three phases:

- Building asset-based threat profiles. (Organizational evaluation)
- Identifying infrastructure vulnerabilities. (Information infrastructure evaluation)
- Developing and planning a security strategy. (Evaluation of risks to the company's critical assets and decision making.)

10. Quantitative Threat Modeling Method

This hybrid method combines attack trees, STRIDE, and CVSS methods. It addresses several pressing issues with threat modeling for cyber-physical systems that contain complex interdependencies in their components. The first step is building components attack trees for the STRIDE categories. These trees illustrate the dependencies in the attack categories and low-level component attributes. Then the CVSS method is applied, calculating the scores for all the tree's components.