

**UNIVERSIDAD TECNOLÓGICA DE**

**SAN LUIS RIO COLORADO**

**Modelado de procesos de amenazas**



**MTRO. AURELIO FLORES**

**ALUMNO: VICTOR MANUEL GALVAN COVARRUBIAS**

**ING. EN DESARROLLO Y GESTIÓN DE SOFTWARE**

San Luis Rio Colorado, Sonora Mayo, 2022

**Methods**

The threats listed above can be prevented using a number of different threat modeling tactics.

**PASTA**

Attack simulation process and threat analysis. It is a seven-step modeling process used to define objectives, requirements, and procedures for security operations. The seven steps are:

• Define objectives

• Define scope

• Application decompensation

• Threat analysis

• Detection of vulnerabilities

• Enumeration of attacks

• Risk analysis

**VAST**

Visual, agile and simple modeling of threats. It is a malleable and scalable modeling process for security planning throughout the software development lifecycle.

It is based on three pillars:

• Automation

• Integration

• Collaboration

VAST can be used for application and operational threat modeling and uses workflow diagrams to illustrate threats, assets, vulnerabilities, and remediation tools in an understandable way.

**Trike**

It focuses on the use of threat models as a risk management tool. Threat models establish the “acceptable” level of risk defined by stakeholders assigned to each asset class. Analysis of the requirements model produces a threat model in which threats are identified and given risk values.

**DREAD**

It is a way of classifying and evaluating security risks into five categories:

• Damage Potential: Classifies the extent of damage resulting from an exploited weakness.

• Reproducibility: Classifies the ease of reproducing an attack.

• Exploitability: Assigns a numerical rating to the effort required to launch the attack.

• Affected Users – A value that represents how many users are affected if an exploit becomes widely available.

• Detectability: Measures how easy it is to discover the threat.

**Attack tree**

The tree is a conceptual diagram showing how an asset or target might be attacked, consisting of a root node, with leaves and child nodes added. Child nodes are conditions that must be met for the direct parent node to be true. Each node is satisfied only with its direct child nodes.

**CVSS**

Common vulnerability scoring system. This method provides a way to capture the main characteristics of a vulnerability and assign a numerical score (ranging from 0 to 10, with 10 being the worst) that shows its severity. The score is then translated into a qualitative representation (eg, low, medium, high, and critical). This representation helps organizations effectively assess and prioritize their unique vulnerability management processes.

**T-MAP**

It is an approach commonly used in commercial off-the-shelf systems to calculate attack path weights. The model incorporates UML class diagrams, including the access class, the vulnerability, the target assets, and the affected value.

**OCTAVE**

It is a risk-based strategic planning and assessment method. OCTAVE focuses on assessing organizational risks only and does not address technology risks. OCTAVE has three phases:

• Asset-based threat profiling.

• Identification of infrastructure vulnerabilities.

• Develop and plan a security strategy.

Quantitative threat modeling method

This hybrid method combines attack trees, STRIDE, and CVSS methods.

* The first step is to build component attack trees for the STRIDE categories. These trees illustrate dependencies on attack categories and low-level component attributes.
* Then the CVSS method is applied, calculating the scores for all the components of the tree.