UNIVERSIDAD TECNOLÓGICA DE SAN LUIS RIO COLORADO

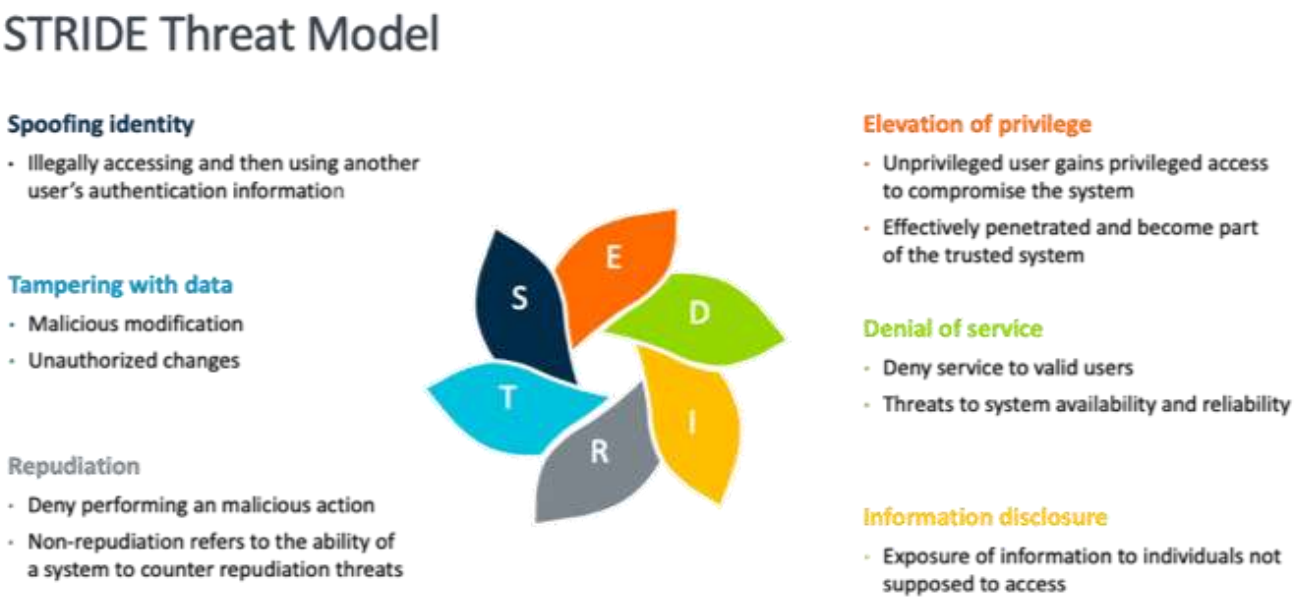
STRIDE investigación

MTRO. AURELIO FLORES

ALUMNO: VICTOR MANUEL GALVAN COVARRUBIAS

ING. EN DESARROLLO Y GESTIÓN DE SOFTWARE

San Luis Rio Colorado, Sonora Mayo, 2022



The STRIDE model, is a threat model created by Praerit Garg and Loren Kohnfelder to identify digital **security threats**.

The STRIDE model involves going through all of a network's processes, data repositories, data flows, and trust boundaries to find threats.

Each threat violates a desired system state, such as:

- **Spoofing violates authenticity.**
- **Tampering violates integrity.**
- **Repudiation violates non-repudiability.**
- **Information disclosure violates confidentiality.**
- **Denial of service violates availability.**
- **Elevation of privilege violates authorization.**

[S]poofing 

Every computer requires user authentication to prevent unauthorized access to confidential data. Stricter systems require multi-factor authentication by asking for a one-time password or personal identification number (PIN) typically sent to the user's mobile device.

User authentication prevents spoofing, which cyber attackers often do to hack into a target system. They often steal an authorized user's password through phishing or keylogging.

[T]ampering

Maintaining system integrity means ensuring that information stored in a computer is real, accurate, and has not been modified.

Imagine if any of the details in a customer's record has been tampered with. A vendor can end up charging him/her for a product/service that he/she didn't purchase. Remediation can mean chargeback fees, issuing apologies, or even getting sued.

[R]epudiation 

No user should ever share his/her username and password with anyone. That's because any transaction made with his/her account is his/her responsibility.

This model ensures repudiation through end-user license agreements (EULAs) that subscribers are asked to accept during signup or registration. That makes the signatory responsible for every activity related to the use of a product/service.

[I]nformation Disclosure

Every employee learns corporate secrets as they grow older in an organization. The higher up the chain you get; the more confidential data you gain access to. But it's only natural for companies to keep proprietary information secret, especially if this has to do with their success.

[D]enegation of Service

We all know by now that a website that goes offline for even a couple of minutes translates to lost sales and business opportunities. That's why threat actors often launch denial-of-service (DoS) attacks on chosen targets.

[E]levation of Privilege

Determining a user's access level to any system is crucial to keeping confidential information protected at all times. Ensuring authorization via the STRIDE model lets an organization prevent elevation or escalation of privilege, which can lead to data theft or breach.

The **STRIDE** model prevents threats, specifically spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege by **making sure that any system maintains authenticity, integrity, non-repudiability, confidentiality, availability, and authorization through the use of strategies.**