Instituto
Politécnico
Nacional

Temas de Tesis

Raúl Acosta Bermejo

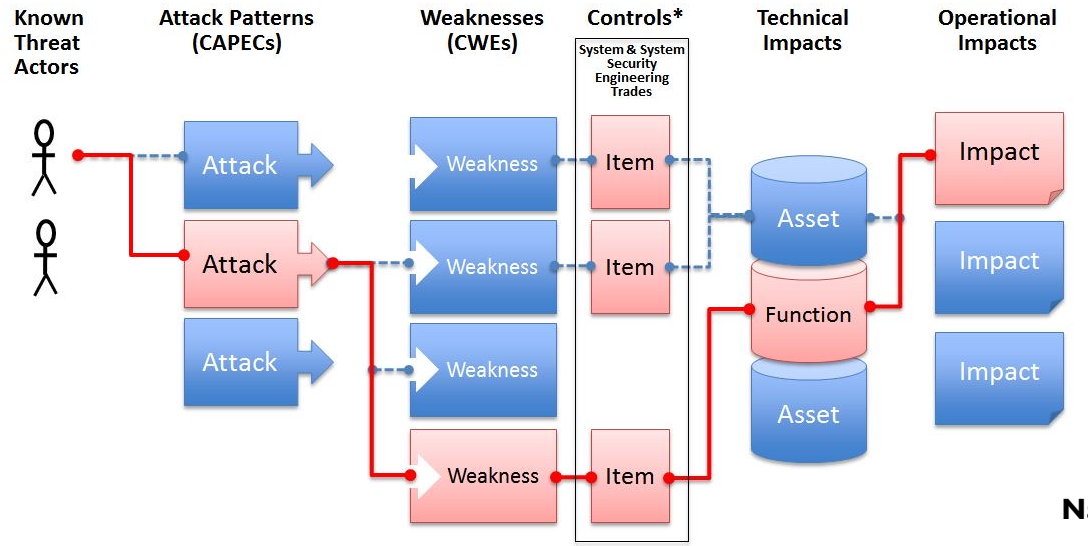
2024-A

Centro de
Investigación en
Computación

Table of contents

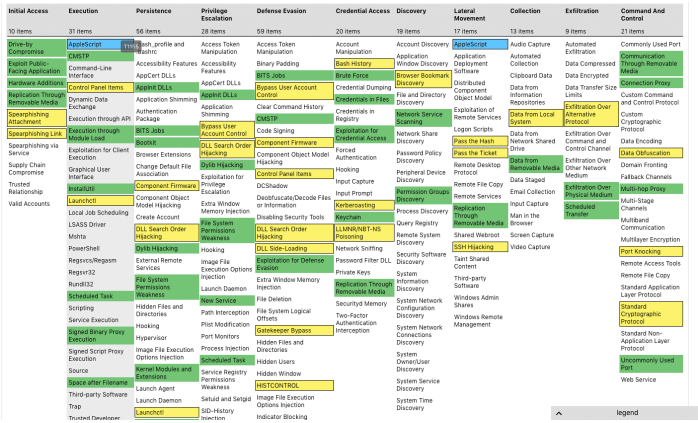
Threats

Engineering for Attacks

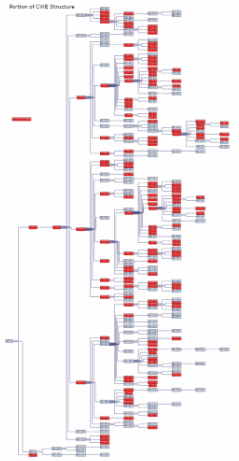


* Controls include architecture choices, design choices, added security functions, activities & processes, physical decomposition choices, code assessments, design reviews, dynamic testing, and pen testing

MITRE ATT&CK



NVD / NIST
National Vulnerability Database



Subject 1: Threat Analysis, Risk Assessment, Modeling threats

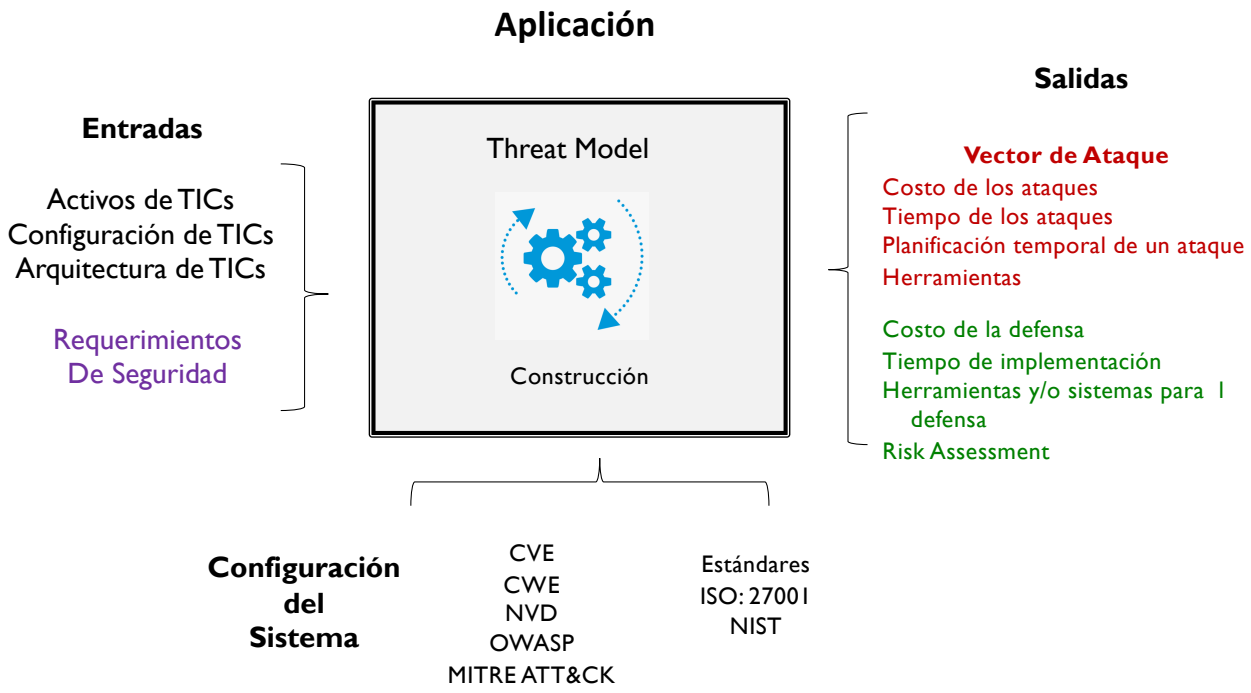
Description

- Attack tree
  - They are conceptual diagrams showing how an asset, or target, might be attacked.
  - What is the cost, time, and probability of an attack?
- Defense Tree
  - Mitigation tree.
  - Attack-defense tree
- Others
  - Fail tree.

Subject 2: Build model

Description

- Proof of Concept(PoC)
- Build a model
  - Dynamic.
- Choose a kind of Test case
  - Cloud.



Malware

- Subjects of Threats
  - Trees, Graphs, etc.

- Subjects of Malware
  - Analysis
  - Detection / Clasification

Malware

- WikiLeaks
  - Julian Assange.
  - 2014 source code and apps
  - https://wikileaks.org/
  - Spyware

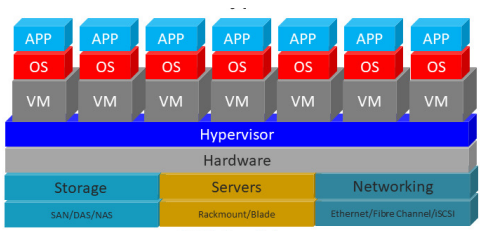
Subject 3: Malware

Description

- Make new classification algorithms using:
  - TTPs
  - IoA (*Indicator Of Activity*)
  - IoC (*Indicator Of Compromise*)
  - YARA rules
- Machine Learning and/or Deep Learning
- Continue with the “Malware Laboratory”

cuckoo

VOLATILITY



Subject 3: Malware

Description

- Make a multi-class classifier of malware samples:
  - SOTA of ML and DL.
  - Create a dataset using MAREA
    - Using windows samples
    - Different types of files.
  - Detect different techniques of Obfuscation
    - Packing and subverting packers like UPX.
    - Hacking File magic numbers.
    - Anti-tamper, anti-debugging
    - Binary or source code obfuscation

      Rename vars, control flow, dummy instructions, etc.
  - Tools needed
    - Malware laboratory.

Obfuscators
For protections of intellectual property

Questions or Comments

Personal Web Page

https://www.cic.ipn.mx/~racostab

Email

racostab@ipn.mx

racostab@cic.ipn.mx

Tel.

55-57-59-60-00

Ext. 56652