



Instituto
Politécnico
Nacional

Temas de Tesis

Raúl Acosta Bermejo
2024-A



Centro de
Investigación en
Computación





Instituto
Politécnico
Nacional

Centro de
Investigación en
Computación



Table of contents

❖ Subjects of **Threats**

- Trees, Graphs, etc.

❖ Subjects of **Malware**

- Analysis
- Detection / Clasification



Engineering for Attacks



Phylogenetic tree of the CBE structure. The tree shows the evolutionary relationships between various CBEs. The root is on the left, and the branches lead to the CBEs on the right. Red bars indicate specific CBEs. The tree is labeled 'Phylogenetic tree of the CBE structure'.

NVD / NIST
National Vulnerability Database





Subject I: Threat Analysis, Risk Assessment, Modeling threats

Description

❖ Attack tree

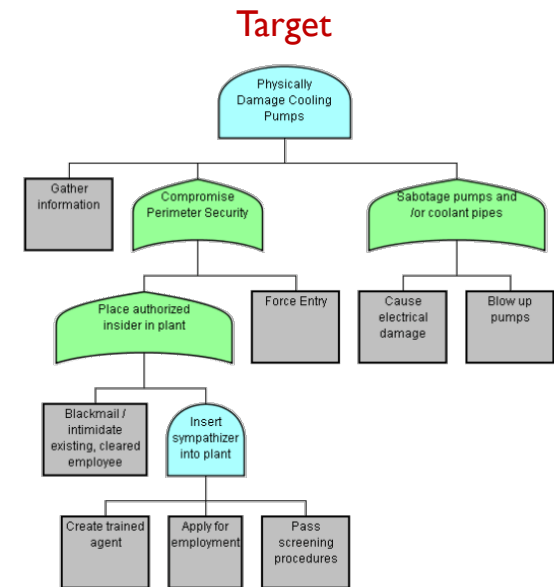
- They are conceptual diagrams showing how an asset, or target, might be attacked.
- What is the cost, time, and probability of an attack?

❖ Defense Tree

- Mitigation tree.
- Attack-defense tree

❖ Others

- Fail tree.

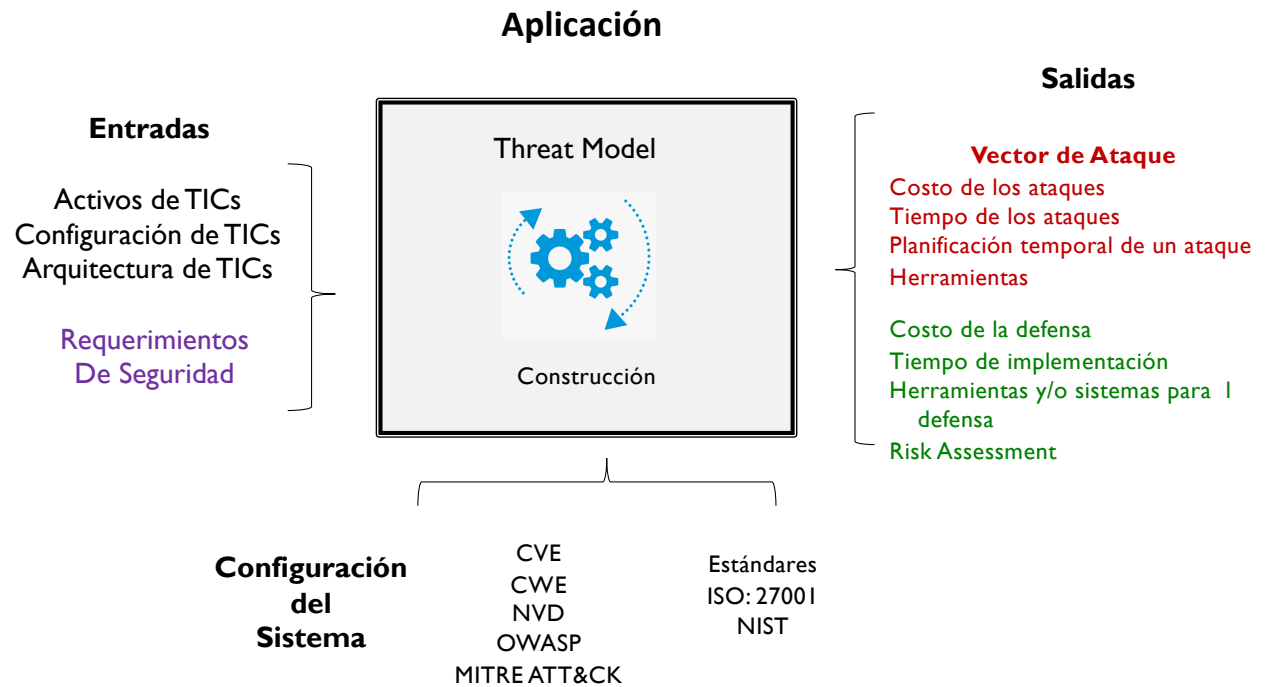




Subject 2: Build model

Description

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





Instituto
Politécnico
Nacional

Centro de
Investigación en
Computación



❖ Subjects of Threats

- Trees, Graphs, etc.

Malware

❖ Subjects of Malware

- Analysis
- Detection / Clasification



Malware

❖ WikiLeaks

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



The WikiLeaks website interface. At the top is the WikiLeaks logo and navigation links: Leaks, News, About, Partners. A search bar, Shop, and Donate buttons are on the right. The main content area features a large graphic of an hourglass with a globe inside, titled 'The Spy Files'. Below this is a text block stating: 'On Thursday, December 1st, 2011 WikiLeaks began publishing *The Spy Files*, thousands of pages and other materials exposing the global mass surveillance industry.'

Below the main content, there is a section titled 'Remote Monitoring & Infection Solutions: FINSPY' with a table of releases.

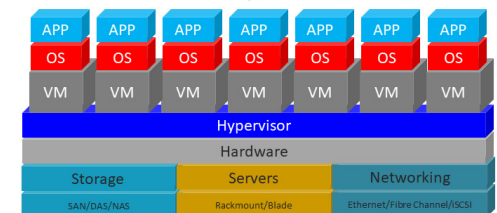
Company	Author	Document Type	Date	Tags
GAMMA		Brochure	2011-10	GAMMA FINFISHER TROJAN

Below the table, there is a download link: 'Download: 289_GAMMA-201110-FinSpy.pdf'. At the bottom, there is a media section with links to 'OWNI', 'Bugged Planet', 'Bureau of Investigative Journalism', and 'Journalism'.





- ❖ 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”





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