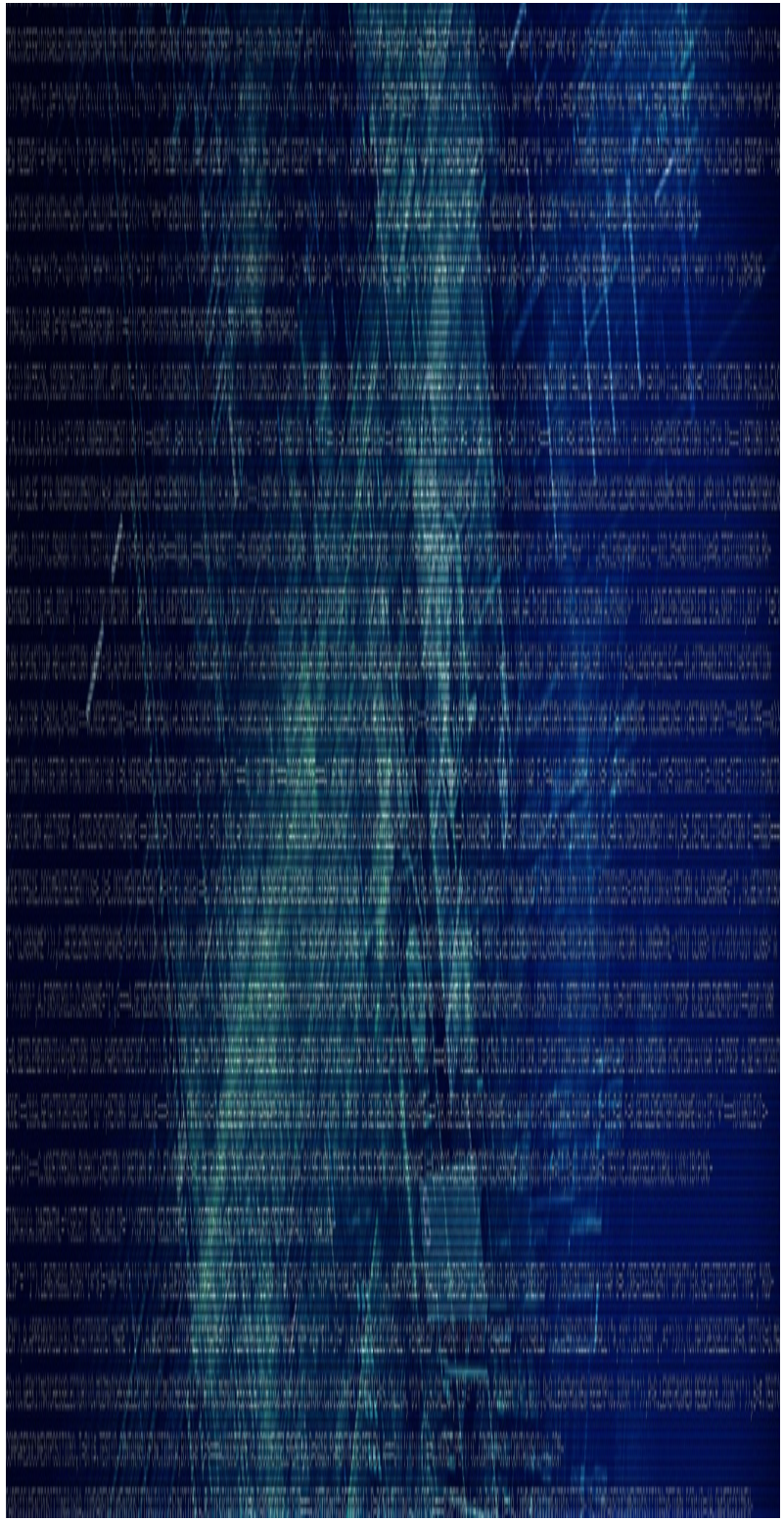
Instituto Politécnico Nacional
Centro de Investigación en Computación
Laboratorio de Ciberseguridad

Temas de Tesis

Raúl Acosta Bermejo

2022-B

14 de octubre del 2022

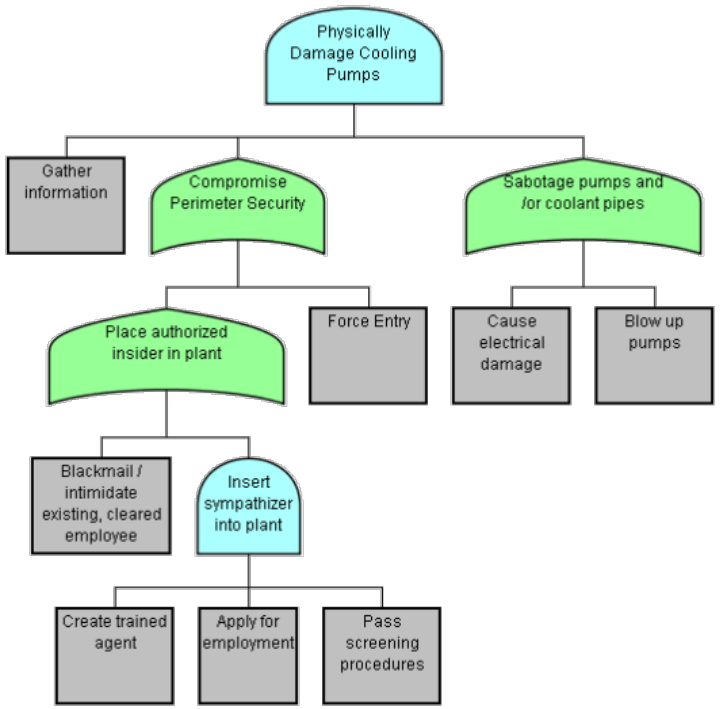


Temas de Tesis 1

Threat Analysis and
Risk Assessment
Modeling threats

Descripción

- Attack tree
  - They are conceptual diagrams showing how an asset, or target, might be attacked..
  - Cual es el costo, tiempo y probabilidad de un ataque?
- Defense Tree
  - Mitigation tree.
  - Attack-defense tree
- Others
  - Fail tree.



Temas de Tesis 1

Aplicaciones reales

- Software comercial
  - Isograph
  - SecurITree/Amenaza.

    Costo de $3,750 a $84,000 USD ($1.68 millones).
  - Cual es el costo, tiempo y probabilidad de un ataque?
- Herramientas similares
  - CAIRIS
    - Comercial, Demo
    - Open Source: https://github.com/cairis-platform/cairis

Temas de Tesis 1

SCOPUS

Attack tree: 12,2k
Computer Science: 5.6k
Biological Sciences: 4k
Engineering: 3k

Conference: 3k, Articles: 2k
2023 (13), 2022 (637), 2021 (906), 2020 (656)

Threat Modeling:
A Summary of Available Methods
SEI: August 2018, White Paper

12 metodos incluidos los árboles

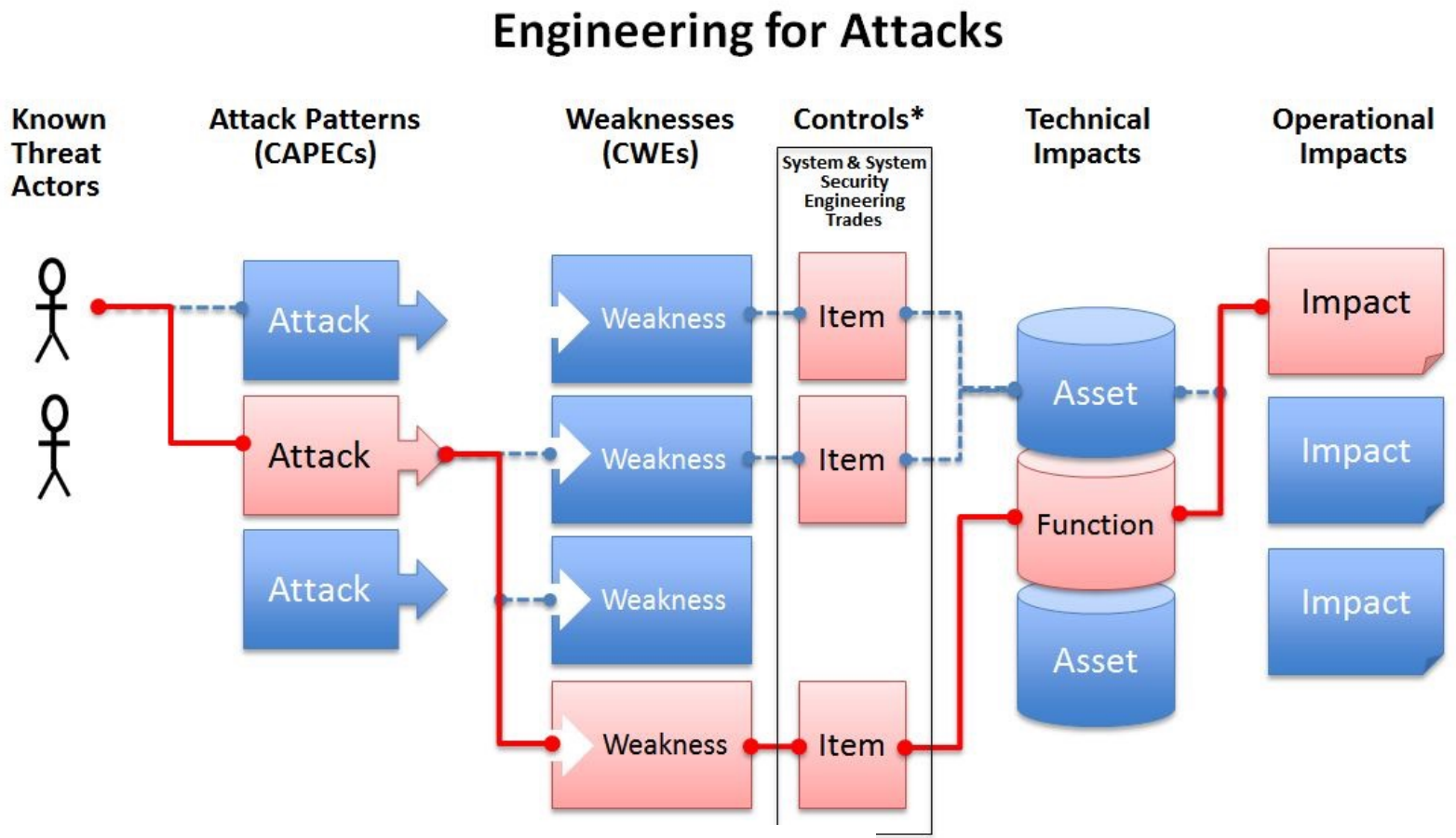
Foundations of Attack–Defense Trees
Barbara Kordy, Sjouke Mauw, Saša Radomirović, Patrick Schweitzer
Conference paper, LNSC,volume 6561.

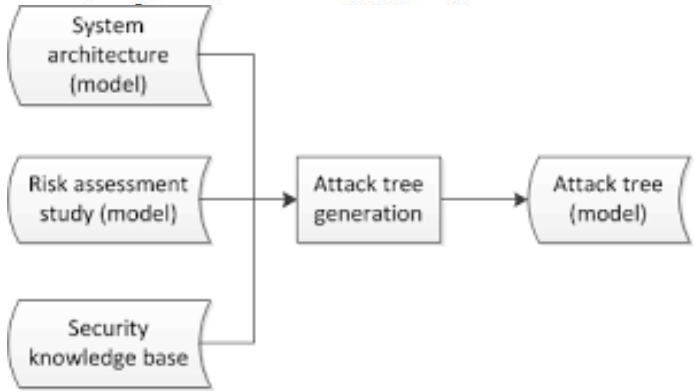
Ejemplos de artículos muy citados

- Scalable, graph-based network vulnerability analysis.
- Model inversion attacks that exploit confidence information and basic countermeasures.
- Dynamic security risk management using Bayesian attack graphs.
- Naive Bayes vs decision trees in intrusion detection systems.
- Cybersecurity for critical infrastructures: Attack and defense modeling.

Exploiting attack–defense trees to find an **optimal** set of countermeasures, IEEE.
A **Minimum** Defense Cost Calculation Method for Attack Defense Trees, Hindawi.

Temas de Tesis 1





TICs graph

Defense tree

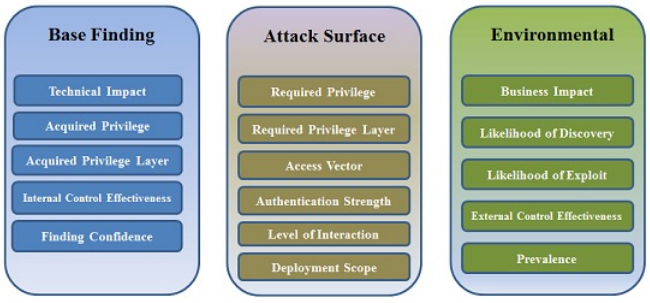
CIS Controls (Critical Security Controls)

CIS Controls Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

Common Weakness Enumeration

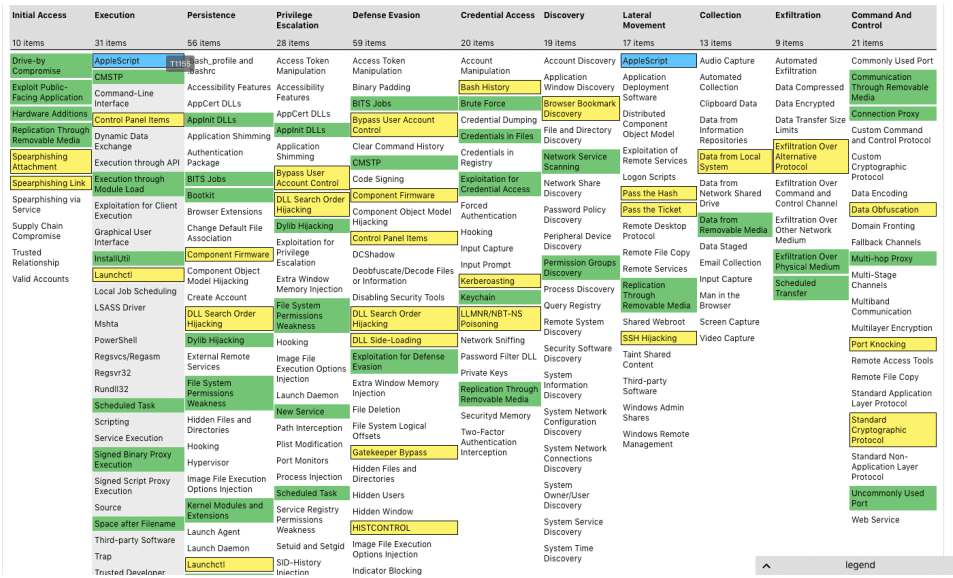
CVE® Common Vulnerabilities and Exposures



INSTITUT
LA TÉCNICA

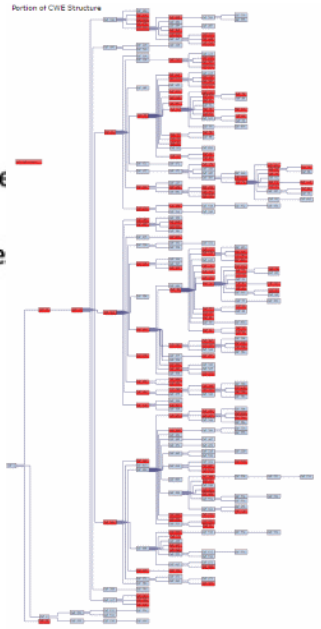
Attack tree

MITRE ATT&CK



A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failure
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failure
A10:2021-Server-Side Request Forgery (SSRF)*

OWASP®



NVD / NIST
National Vulnerability Database

Objetivos

- Prototipo, PoC (Proof of Concept)
- Centrado en el modelo (gráfico) y no en la GUI.
- Elegir un Caso(s) de Prueba
  App en la Nube? Security by Design?

Problemas

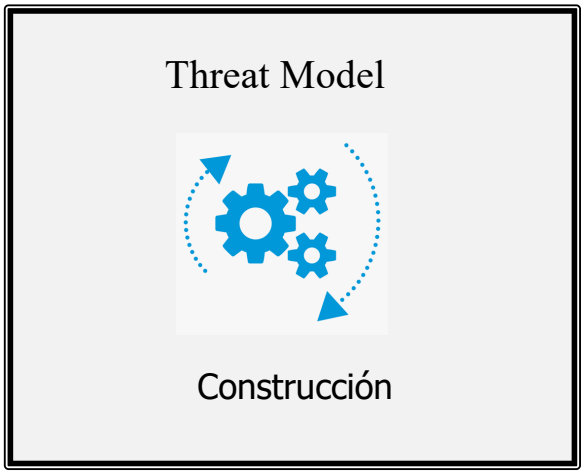
- Como abordar la complejidad de los sistemas?
  Modelo a capas, encapsulación, etc.
- Usar funciones multi-objetivo sencillas.

Aplicación

Entradas

Activos de TICs
Configuración de TICs
Arquitectura de TICs

Requerimientos
De Seguridad



Salidas

Vector de Ataque
Costo de los ataques
Tiempo de los ataques
Planificación temporal de un ataque
Herramientas

Costo de la defensa
Tiempo de implementación
Herramientas y/o sistemas para la defensa
Risk Assessment

Configuración del Sistema

CVE
CWE
NVD
OWASP
MITRE ATT&CK

Estándares
ISO: 27001
NIST

Herramientas
Static Application Security Testing (SAST) Tools
Dynamic Application Security Testing (DAST) Tools

INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA

Gracias

Preguntas o comentarios

Sitio web personal
https://www.cic.ipn.mx/~racostab
Email
racostab@ipn.mx
racostab@cic.ipn.mx
Tel.
55-57-59-60-00
Ext.56652