Centro de
Investigación en
Computación

Análisis de Amenazas

Estándares

Definitions

Research

Course

Análisis y Detección de Malware

Instructor

Acosta Bermejo Raúl

Lecture notes

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción

   Motivación, Ataque/Defensa, Bibliografía
2. Contramedidas
   1. Árboles de ataque
3. Varios temas

   Soluciones (Software/papers)

Introduction

Introducción

Introduction

Motivación

Objetivo

- En esta unidad se verán algunas estrategias que han sido creadas para diseñar contramedidas en ambos sentidos de los actors, es decir, en Ataque y Defensa.
- Se verá primero que es una contramedida y luego como se construye.

Countermeasure

Contramedidas

Contra-inteligencia

Countermeasure

Contrainteligencia

- La Contrainteligencia es el conjunto de actividades destinadas a **anular la eficacia de las acciones de Inteligencia hostiles** y a proteger la información contra el espionaje, el personal contra la subversión, y las instalaciones y el material contra el sabotaje.
- Dichas actividades consisten en el estudio, adopción y aplicación de un conjunto de medidas cuya eficacia dependerá, fundamentalmente, del **conocimiento que se tenga del enemigo** y de sus posibilidades.

Countermeasure

Técnicas usadas por el malware

Countermeasure used by malware

- To evade the detection by antivirus scanners.
- Obfuscation
  - Payload encryption.
  - Packers.- A tool used to compress and scramble an EXE file. Used to hide the malicious nature of malware and thwart analysis by researchers.
  - Polymorphism and Metamorphism malware.
- Detecting that the malware is running inside a VM o sandbox environment.

Countermeasure

Clasificación

We could classify anti-analysis tricks (done by malware) in three big groups:

- **Anti Virtual Machine**, that tries to detect if the execution environment is a known VM or emulator.
- **Anti Debugging**, that tries to detect if the program is running under the surveillance of a debugger.
- **Anti Sandbox**, that tries to detect known sandboxing products.

But an scanner can analyse a possible malware to detect:

- Presence of instructions that check a particular sandbox (sbiedll.dll for Sandboxie)
- Some particular values of the system (identificators for hard disks that are read from, e.g. Windows registry).
- Instructions (functions in the API of MS Windows system) to detect debugging. For instance, using the functions IsDebuggerPresent and GetProcAddress.

Attack Tree

Árboles de Ataque

Contra-inteligencia

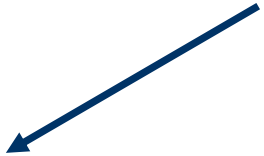
Attack Tree

Introducción

Campo semántico

Risk Analysis

Threat Modelling



Attack Threat Modelling

Phisical Security

Anti-tamper

Classifying threats
STRIDE

Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege

Attack Tree

Introducción

Definitions

- A branching, hierarchical data structure that represents a set of potential approaches to achieving an event in which system security is penetrated or compromised in a specified way. [Moor].
- Attack trees (known as threat trees by Microsoft) provide a formal, methodical way of describing the security of systems based on various attacks [Schneier 99].
  - The root node of the tree is the attackers goal (known as threat by Microsoft), and the children of each node describe a lower-level way of achieving the goal of the parent node.
  - In this manner, the leaf nodes generally contain relatively low-level tasks such as install a key logger on target machine, and the root node contains a goal such as obtain administrators password.

Attack Tree

Introducción

Definiciones

- Estructura de datos en forma de árbol donde a partir de un objetivo final (representado como la raíz) se identifican (como ramificaciones) objetivos secundarios que nos permitirían alcanzar el objetivo final.
  - Los árboles de ataque se utilizan para modelar las posibles vías por las que puede perpetrarse un ataque.

- Referencias
  - Glosario de términos
    - https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=72.html
  - Software
    - https://www.amenaza.com/.

Attack Tree

Introducción

Referencias

- Glosario de términos
  - https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=72.html
- Software
  - Comercial y/o demo por tiempo
    - https://www.amenaza.com/.
  - Open source
    - Muy sencillo: https://satoss.uni.lu/members/piotr/adtool/

Attack Tree

Introducción

Construcción

- El árbol más básico tiene en los nodos internos:
  - Compuertas AND
  - Compuertas OR
  - Compiertas XOR
- En modelos más complejos se usan otras relaciones:
  - SAND: Los hijos se ejecuta de forma secuencial de izq a der.
  - SOR: Igual que el anterior y no evalua todo.
  - PAND: Todos los hijos se inicializan y se Propaga la disrupción.
  - FDEP, SPARE, etc
- Pueden acompañarse de información adicional como:
  - Tiempo de ejecución
  - Costo del ataque

SAND attack tree

Attack Tree

Introducción

Basic examples

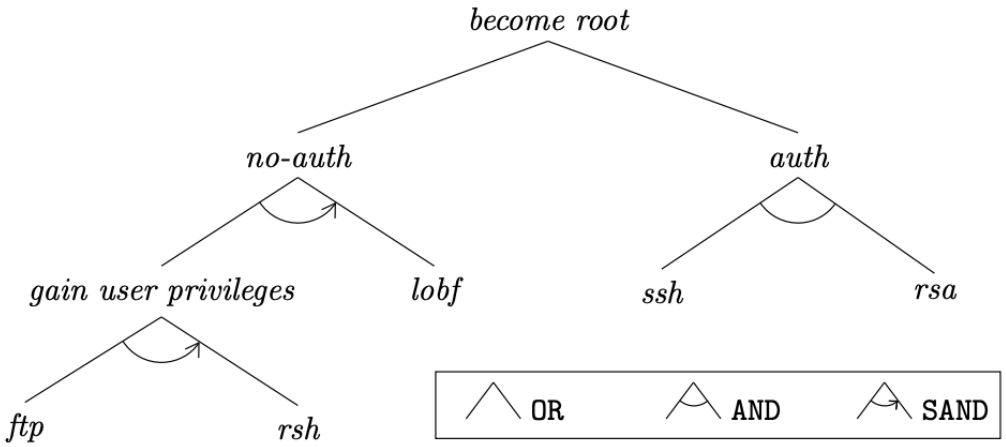


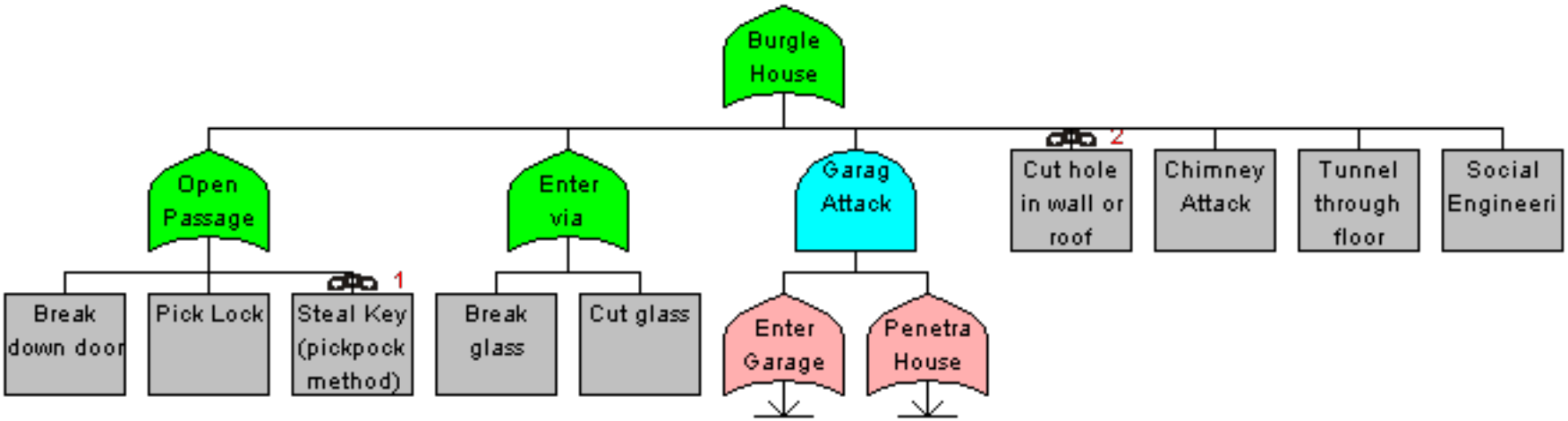
Fig. 1. An attack tree with sequential and parallel conjunctions

Attack Tree

Introducción

Ejemplos

- Robo a una casa



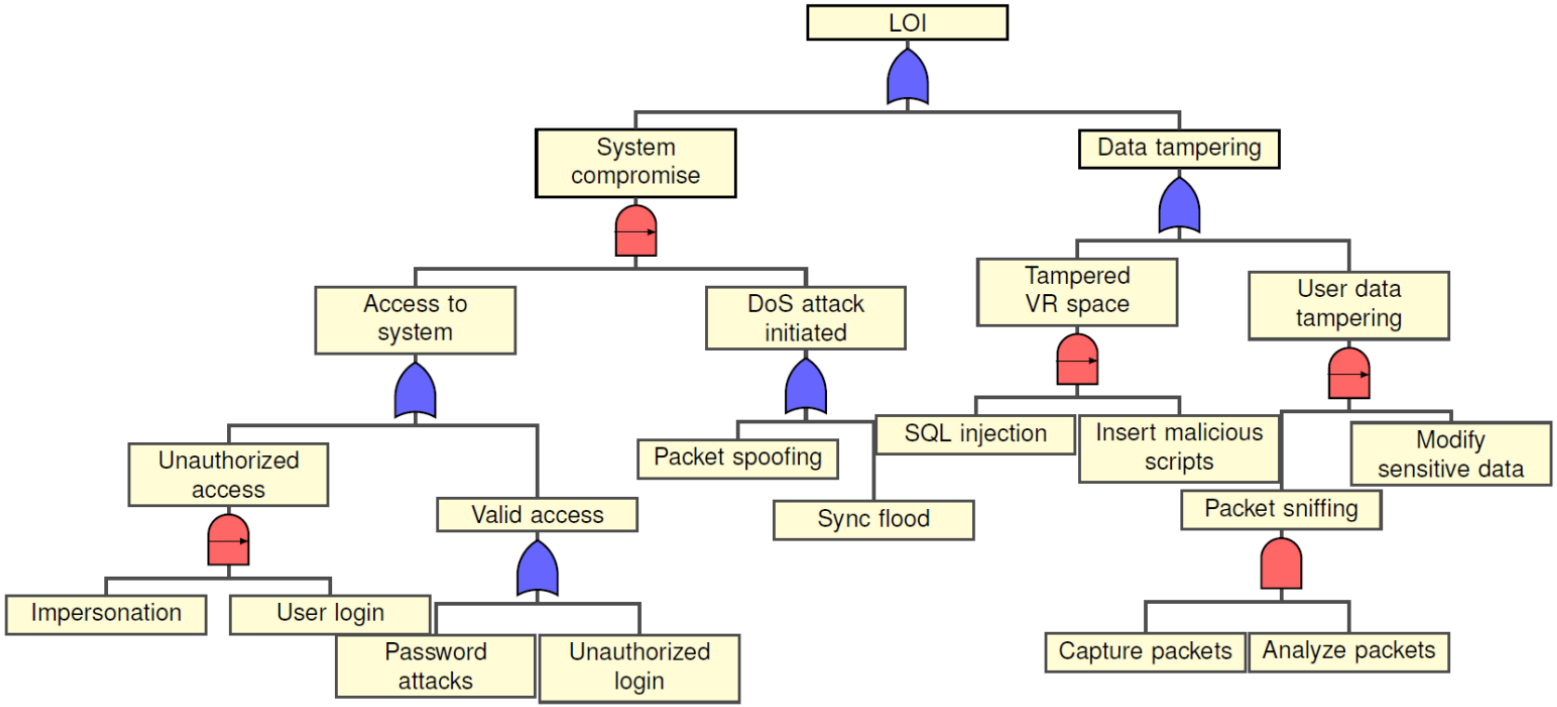
Attack Tree

Introducción

Fuente
Attack Trees for Security and Privacy in Social Virtual Reality Learning Environments, Samaikya Valluripally et al, 2019.

Ejemplos

- Reducing the probability of Loss of Integrity (LoI)



Attack Tree

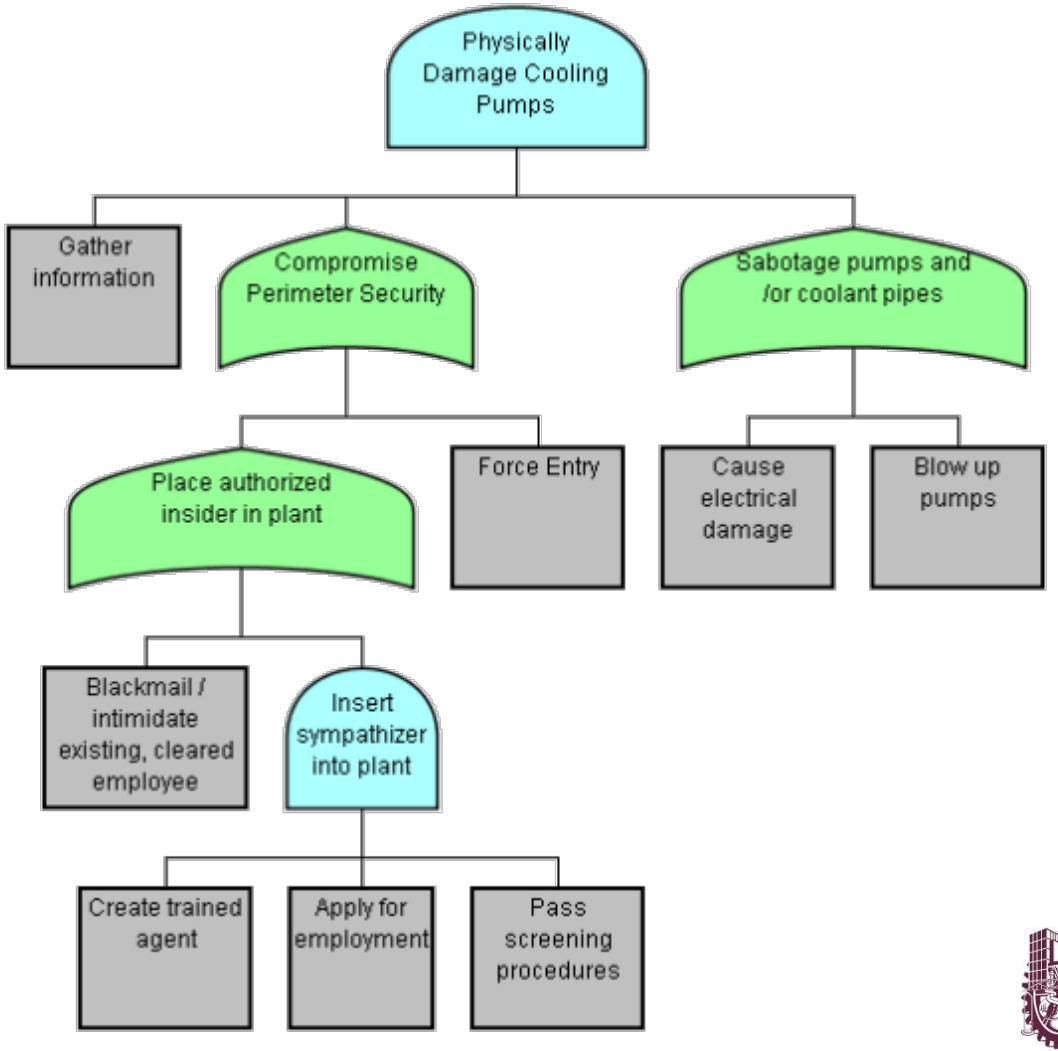
Introducción

Ejemplos

- Ataque a una empresa:

  Transporte de:

  Gas, gasolina, etc.

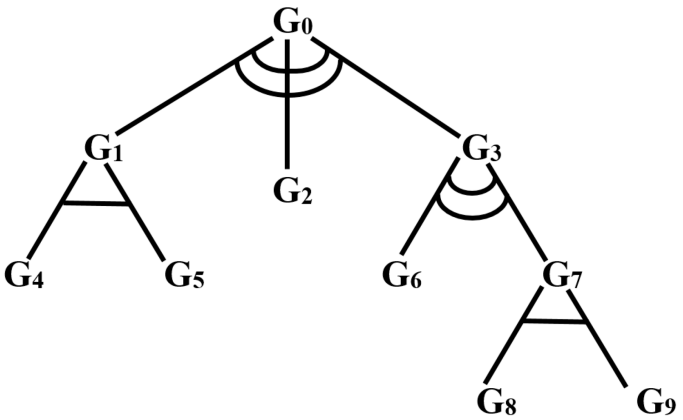


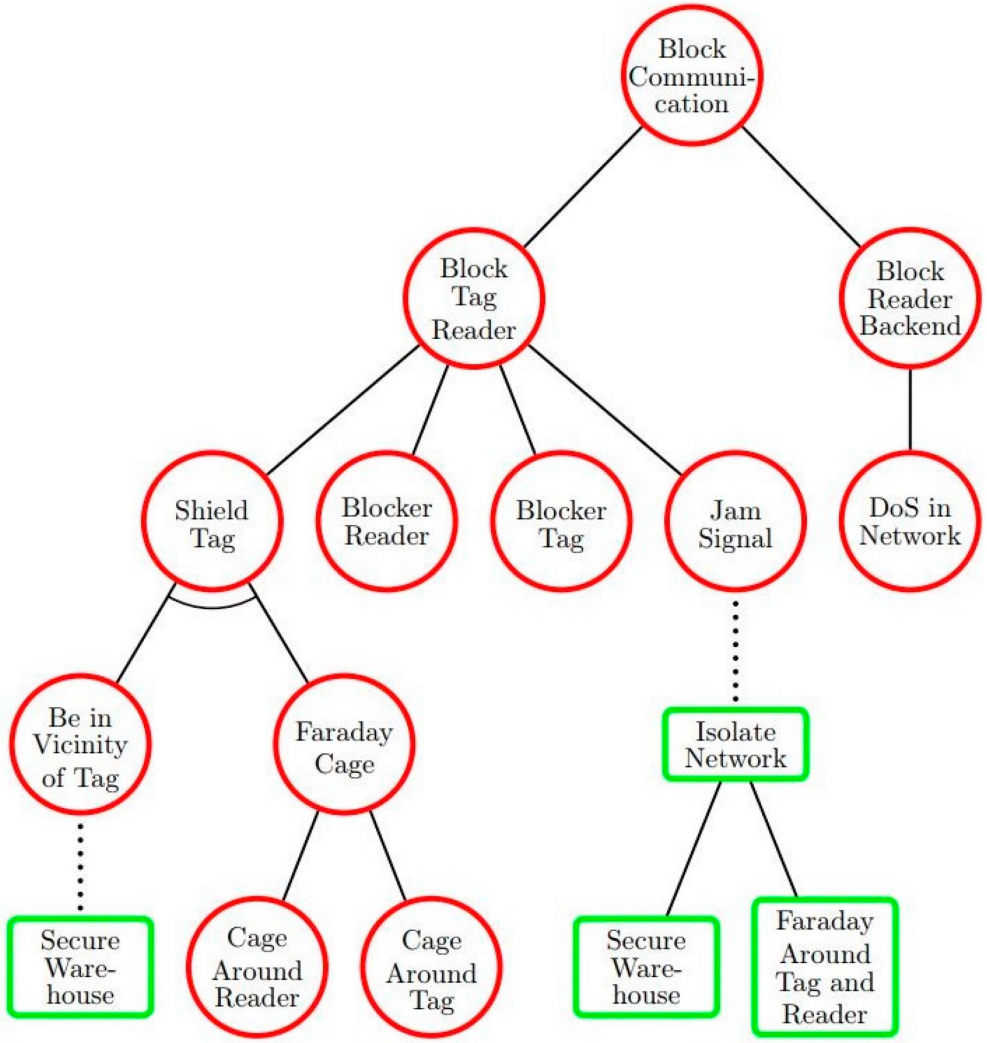
Attack Tree

Introducción

Artículo

- Method for Attack Tree Data Transformation and Import Into IT Risk Analysis Expert Systems. Donatas Viktus **et al**.

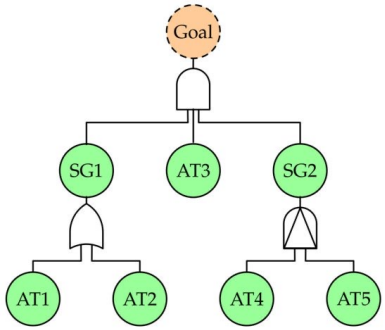




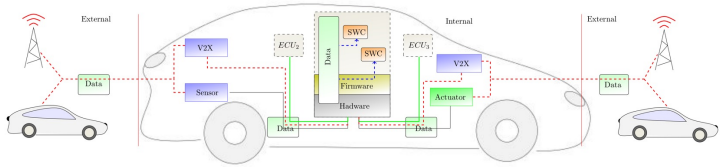
Attack Tree

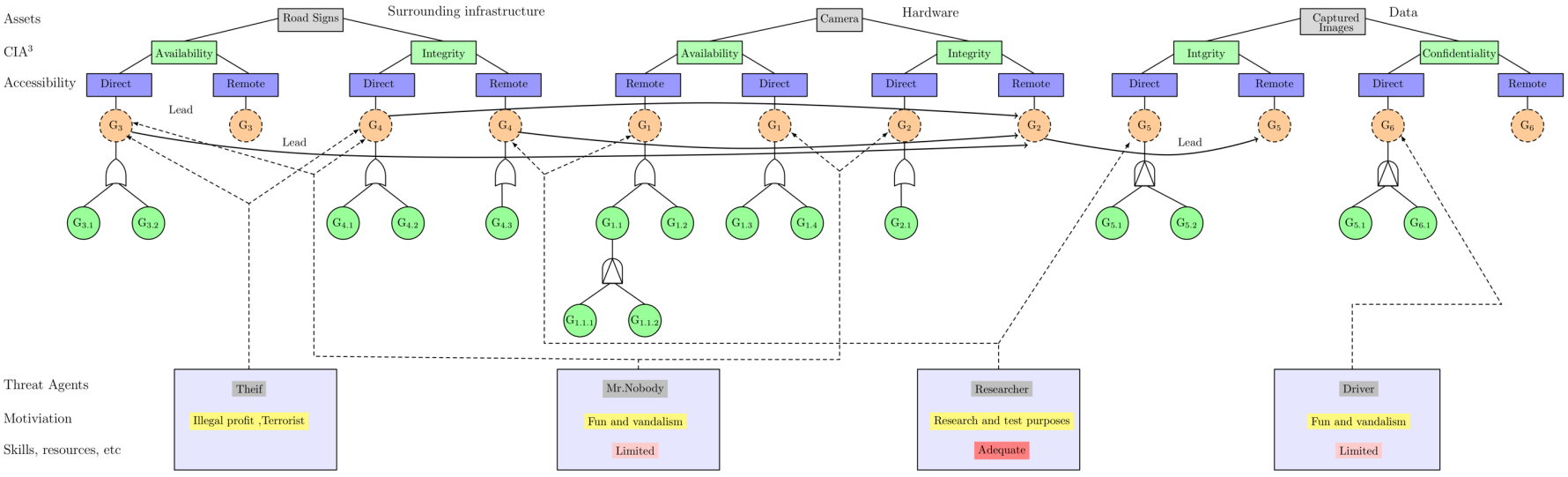
Introducción

Fuente
SAVTA: A Hybrid Vehicular Threat Model: Overview and Case Study.



Assets of the automotive system

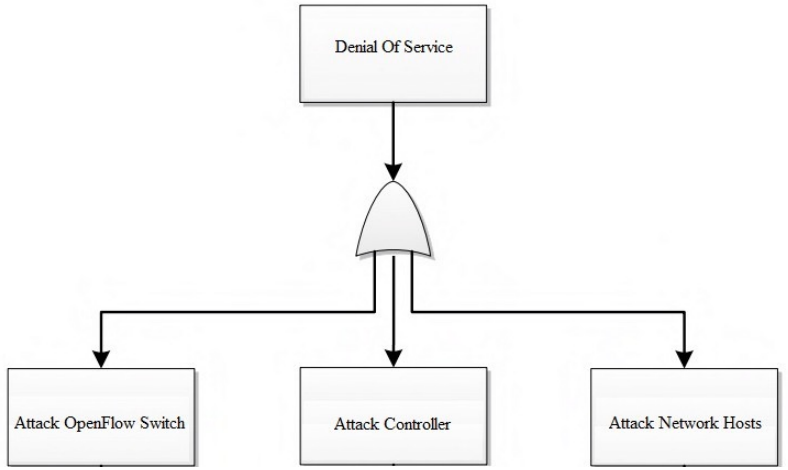


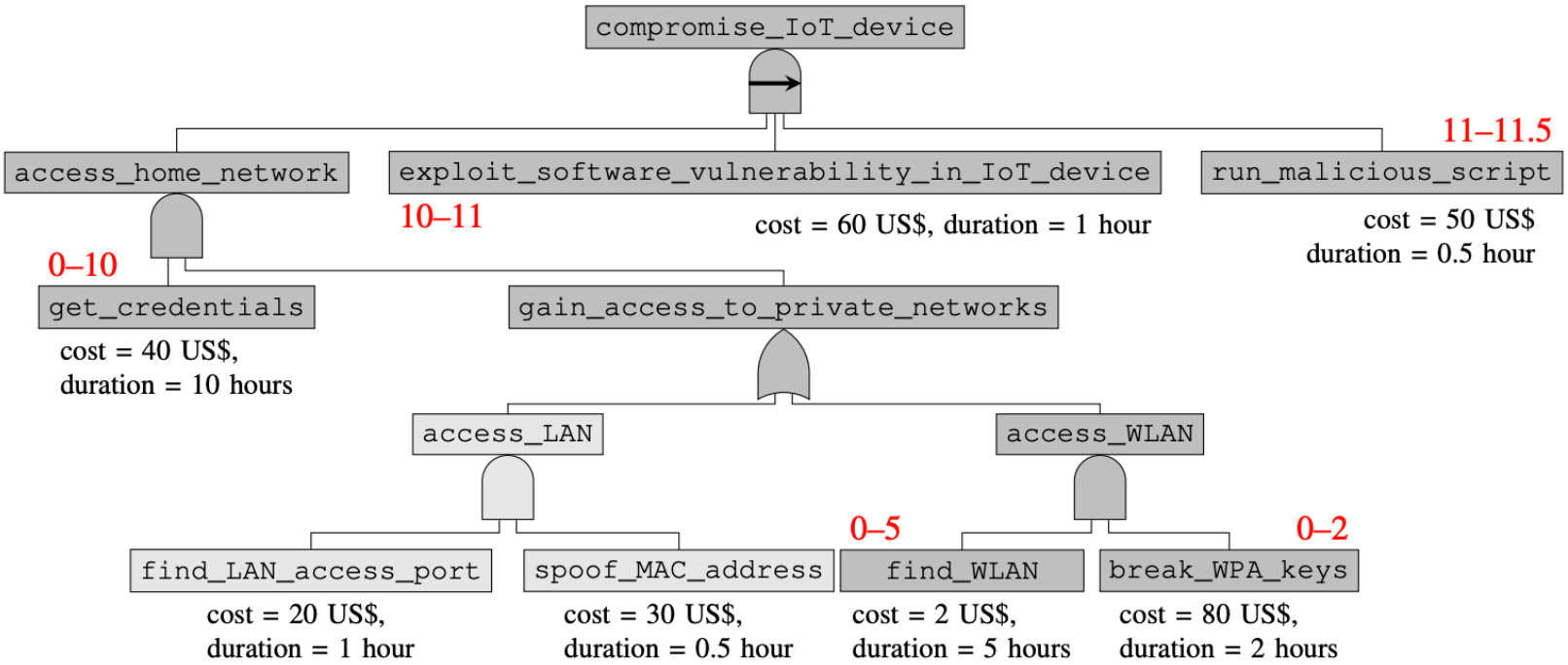


Attack Tree

Introducción

Examples





Attack Tree

Introducción

Variants

- Probabilistic attack tree

  Read the paper: *An Algorithm to Find Optimal Attack Paths in Nondeterministic Scenarios, Carlos Sarraute et al, 2013*.
- Defense tree
- Attack-defense tree
- Fault tree
- Supply Chain Attacks

Attack Tree

Introducción

Tarea obligatoria

- Elaborar un árbol de ataque
  - Por equipos de 3.
  - Tomar como objetivo un activo de IT de ESCOM.
  - Acordar con los demás equipos el objetivo para que no se repita.
  - Entregar un documento que contenga todo el desarrollo y no sólo el árbol:
    - Por que eligieron ese objetivo: que valor tiene?
    - A quien consultaron para saber que ramas tiene el árbol? A parte de las que se les pueden ocurrir a ustedes.
    - Que medidas de protección existen? Verificadas.
  - Si el árbol tiene muchos niveles y/o información (es lo ideal) usar alguna herramienta especializada.

Attack Tree

Introducción

Conclusions

- Attack trees provide a formal methodology for analyzing the security of systems and subsystems.
- They provide a way to think about security, to capture and reuse expertise about security, and to respond to changes in security.
- Security is not a product—it's a process. Attack trees form the basis of understanding that process.

Moving Target Defenses MTD

Defensas basada en Movimiento del Objetivo

Teoría

MTD

Introducción

Definitions

- They are a collection of technologies that seek to improve security and increase resilience and availability of an application through increasing diversity of software and network paths.
- Taxonomy
  - Dynamic runtime environment
  - Dynamic software
  - Dynamic data
  - Dynamic platform
  - Dynamic networks

MTD

Introducción

Implementations

- Multiple OS Rotational Environment (MORE)
  - Operating systems are a significant attack vector for would-be malicious actors in cyberspace. Of particular concern are zero-day vulnerabilities.
- Dynamic Application Rotation Environment (DARE)
  - Owing to the ubiquity of web applications in modern computing, the server software that delivers applications is an attractive attack vector for would-be malicious actors in cyberspace. DARE uses the two most common and freely available web servers: Apache and Nginx.
- Stream Splitting MTD
  - Cyber infrastructures can be attacked with relative ease, as most of the current infrastructures have configurations with a single, static network stream for communication between any two nodes at a particular time.

MTD

Introducción

Implementations

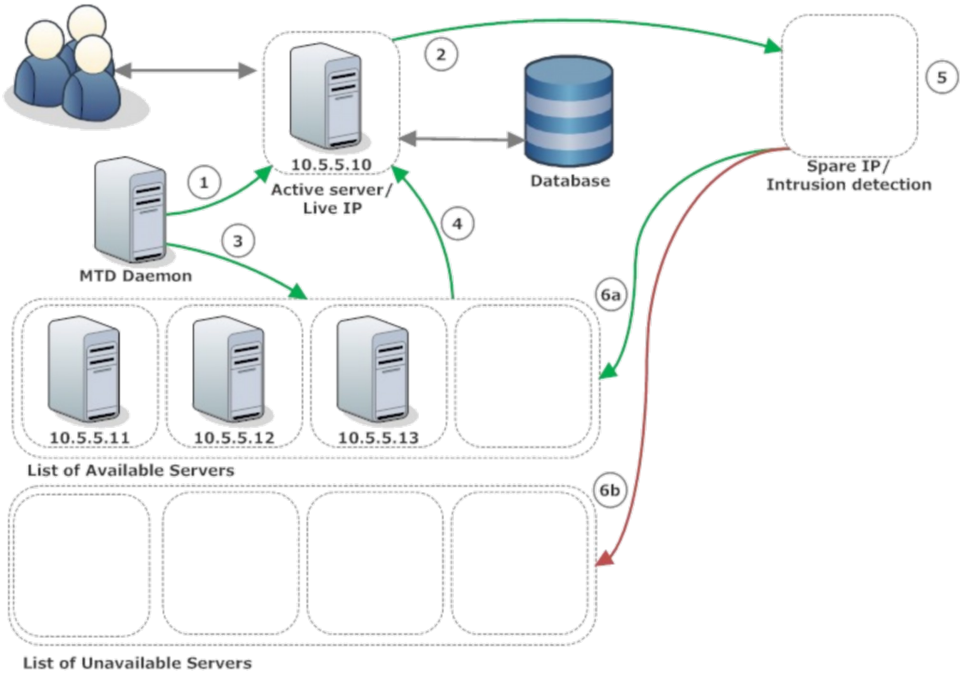
- Software Defined Networking Multiple Operating System Rotational Environment (SMORE)
  - It defends against zero-day cybersecurity attacks by using software-defined networking to manipulate network paths that service user requests. By randomly selecting which server and service will respond to a given user's request, SMORE-MTD makes it more difficult for an attacker to perform reconnaissance and identify which services to attack. SMORE-MTD also increases resilience to vulnerabilities by not guaranteeing that an attacker exploit will be routed to the vulnerable software. .
- Honeybadger MTD
  - It proactive defense uses a software defined networking (SDN) switch to analyze user traffic and divert attacker traffic to a honeypot network to limit their interaction with and possible exploit of vulnerable production servers. By placing a SDN switch in front of a production server, we can programmatically control the flow of packets between a server and its clients.

MTD

Introducción

Implementations

- Multiple OS Rotational Environment (MORE)

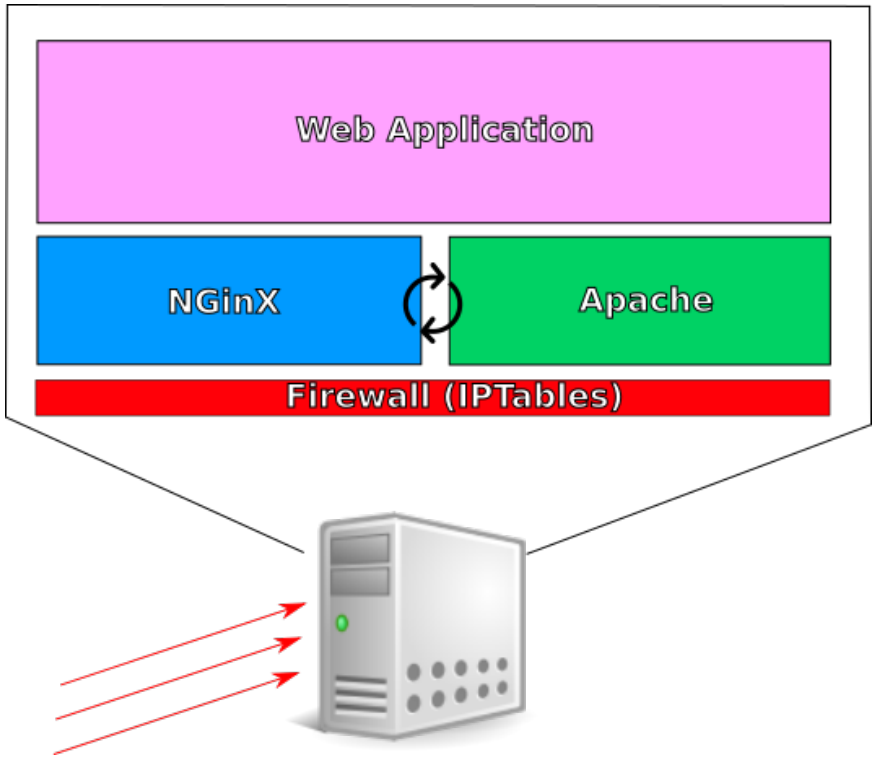


MTD

Introducción

Implementations

- Dynamic Application Rotation Environment (DARE)

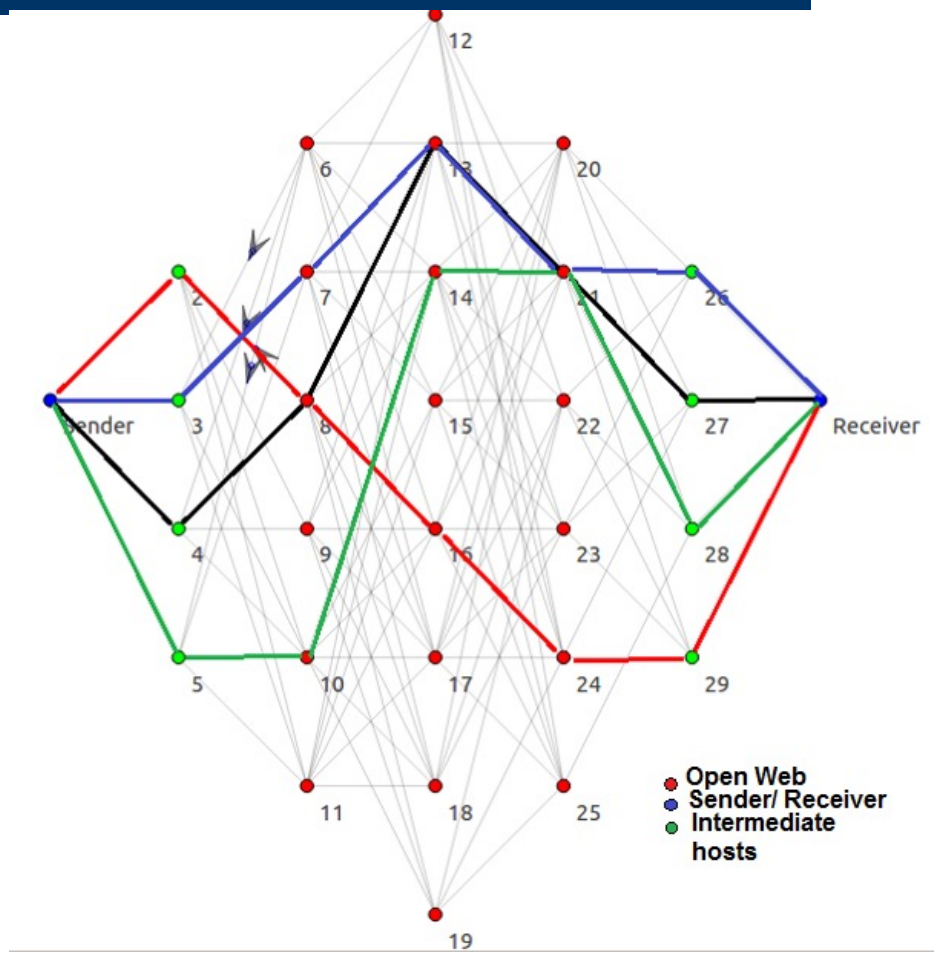


MTD

Introducción

Implementations

- Stream Splitting MTD

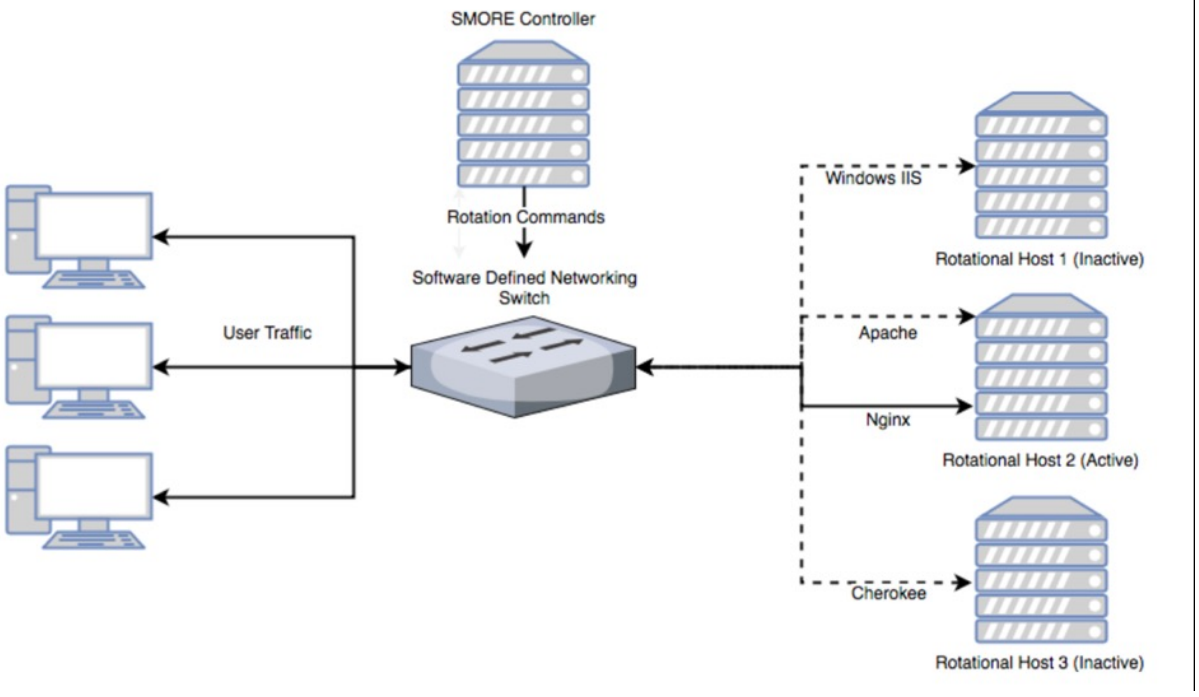


MTD

Introducción

Implementations

- SDN Multiple Operating System Rotational Environment (SMORE)

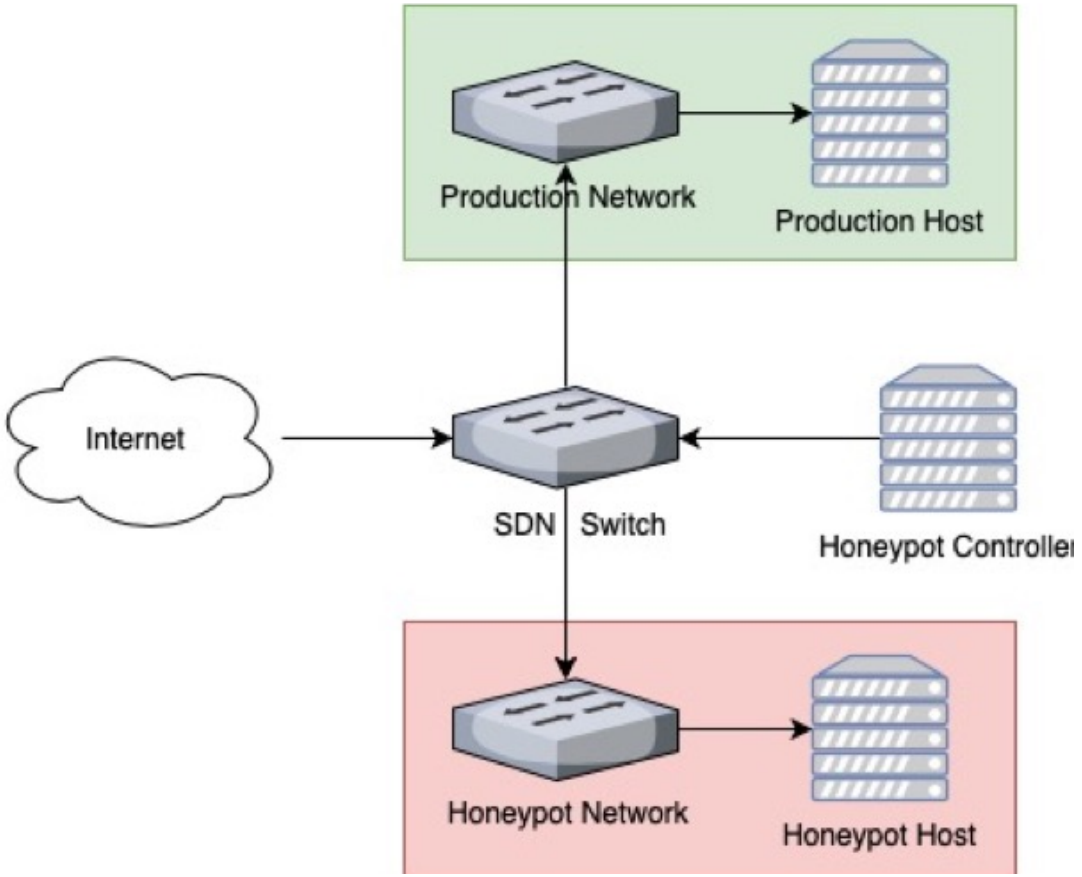


MTD

Introducción

Implementations

- Honeybadger MTD



MTD

Introducción

References

- https://coar.risc.anl.gov/research/moving-target-defense/.
- https://www.sciencedirect.com/topics/computer-science/moving-target-defense.
- .

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652