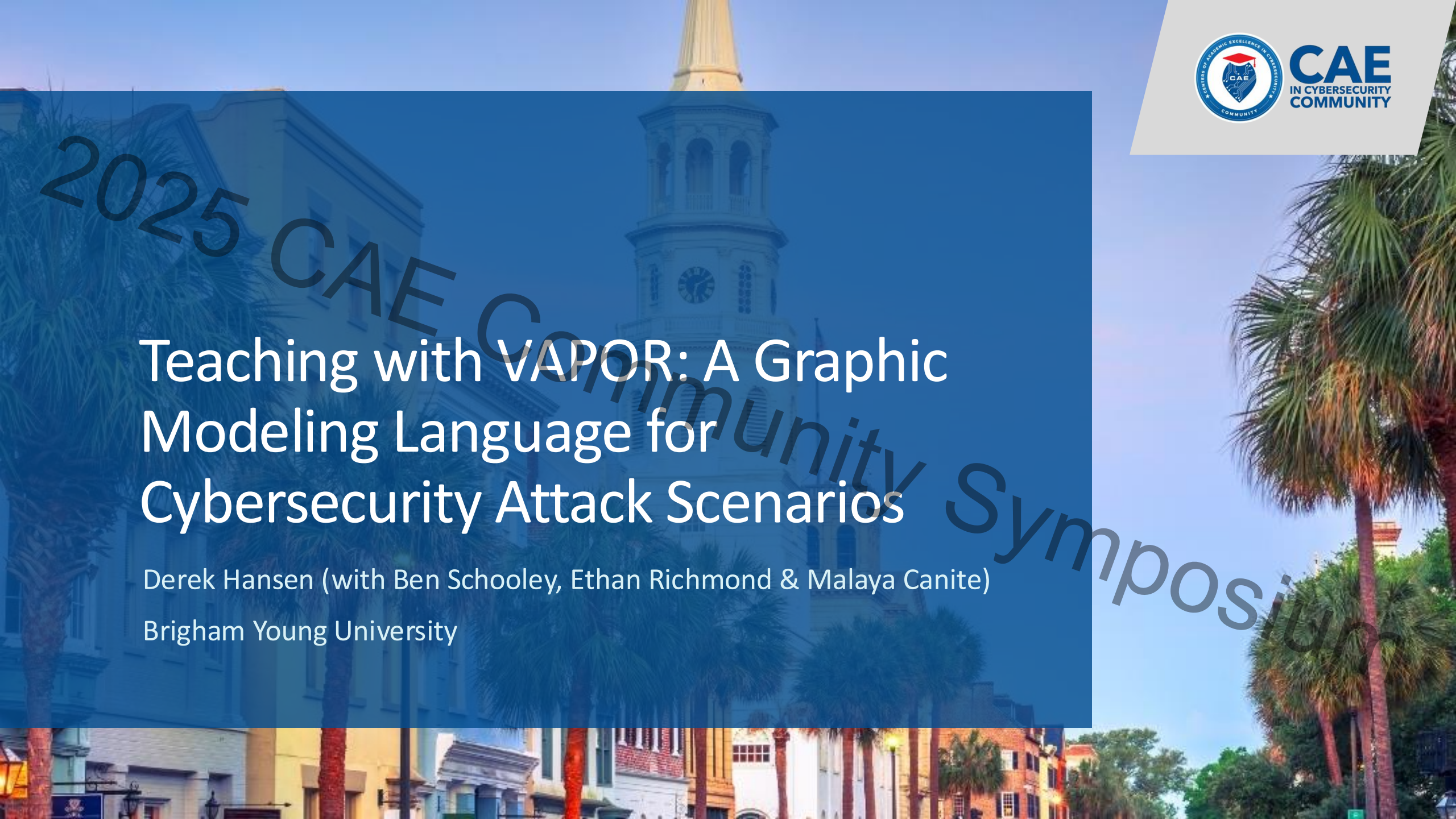


Teaching with VAPOR: A Graphic Modeling Language for Cybersecurity Attack Scenarios

Derek Hansen (with Ben Schooley, Ethan Richmond & Malaya Canite)

Brigham Young University

What is VAPOR & why use it?

VAPOR is a **visual modeling language for cyber attack scenarios** designed to:

- Facilitate learning of adversarial mindset via visualization
- Communicate complex scenarios to different stakeholders
- Show context surrounding attacks

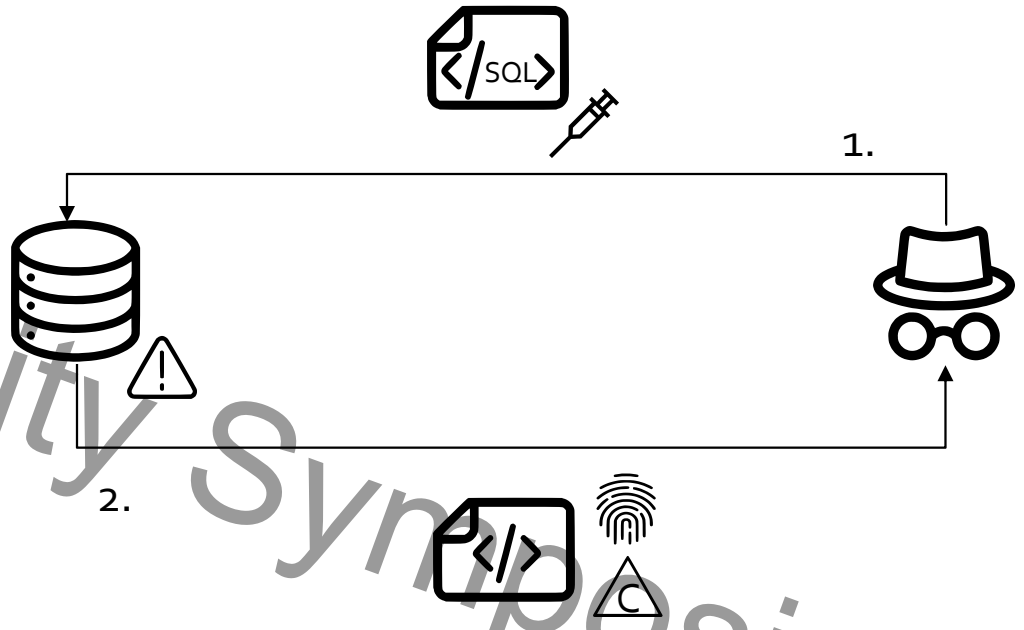
2025 CAE Community Symposium

VAPOR RULES

Components and rules for diagrams

Diagram Components

1. Arrows
2. Containers
3. Objects
   a) Actors
   b) Things
4. Annotations
   a) Actions
   b) States
   c) Components



SQL Injection Exfiltration Example

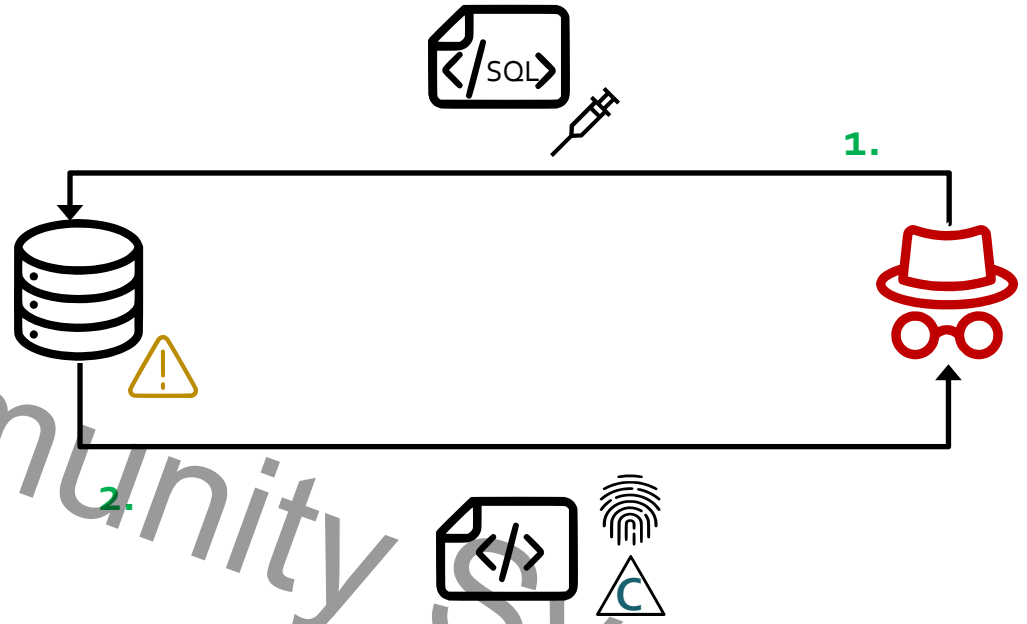
Objective: Extract private customer info

CIA Violation: **Confidentiality**

Attack Type: SQL Injection

Steps:

1. An **attacker** injects malicious SQL code into company ABC's **vulnerable** database.
2. Private customer information is extracted and sent back to the hacker



Description:

An attacker wants to see private customer info. The attacker is aware that Company ABC has a vulnerability on their database, allowing for SQL injection. By exploiting this vulnerability, the attacker gains access to private customer data, breaching confidentiality.

Social Engineering Example Scenario

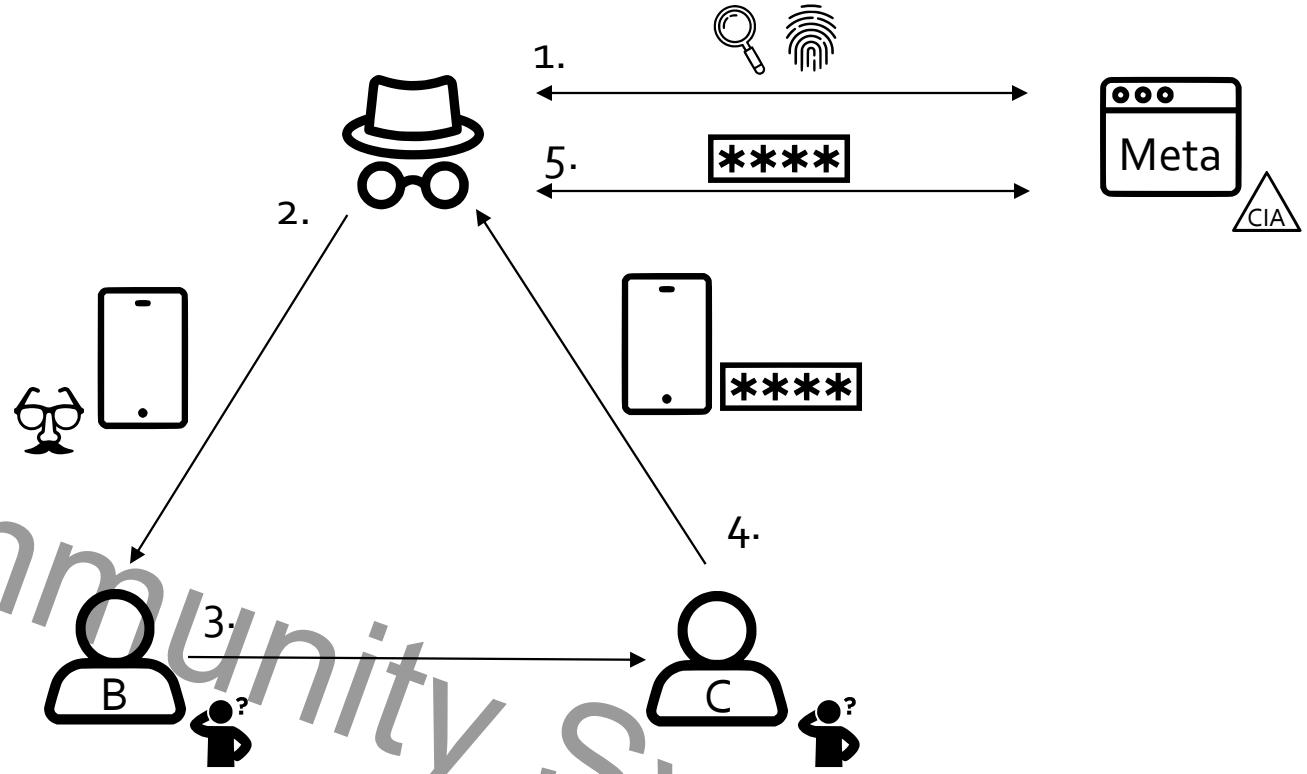
Objective: Take over Erica's account

CIA Violation: Confidentiality, Integrity, Availability

Attack Type: Social-Engineering

Steps:

1. Anna OSINTs Eric's Meta profile, finding info about her and her close friend, Ben.
2. Anna contacts Ben via a "friends" phone, pretending she is Erica and has been locked out of her account.
3. Ben falls for the message, telling Erica's brother, Charlie to send the password to Erica.
4. Charlie reads off Erica's password to Anna via the "friends" phone number in plaintext.
5. Anna can log into Erica's account, tamper, and lock her out.



Description:

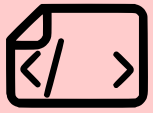
Anna wants to steal Erica's Meta account. She goes on Meta and browses her account, finding info about Erica and her closest friends. Using this information, she contacts her friends, pretending that she's Erica and has been locked out of her account. Under the guise of being Erica, Anna gains Erica's password, which she uses to modify posts and lock her out.

VAPOR Rules

- Always include:
  - Written Scenario
  - Numbered Steps with explanations
  - CIA Triad to show “impact” of attack
  - Attacker
  - Vulnerable or User Error icons
- Use Containers for multi-part attacks
- Use double sided arrows when interaction goes both ways

Customize Empty Icons

BAD

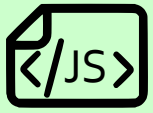


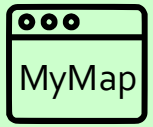
If empty, use Generic File

Limit letters to C, I, or A

Shrink font size to fit empty icons

GOOD



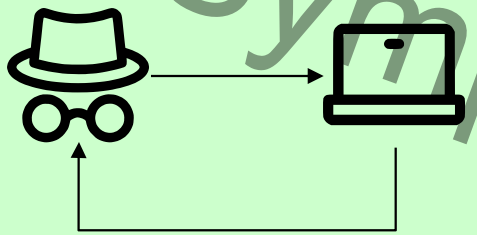


Avoid Duplications of the Same Object

BAD

Redundant

GOOD



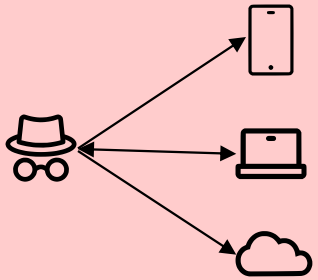
Label & Name Actors If They Are Used Multiple Times

BAD

Who is who?

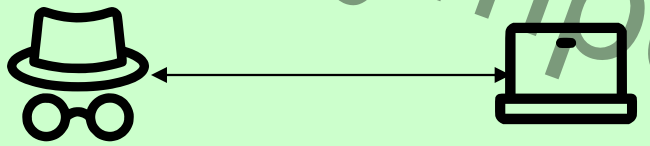
GOOD

Only Include Important Parts of an Attack



Unnecessary

(Hacker checks all, but ultimately interacts with the computer)



2025 CAE Community Symposium

Icon Library

Copy & Paste Icons onto template to create VAPOR diagrams

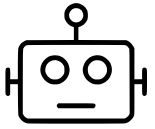
Objects: Actors

User

Protector

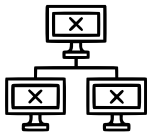
Attacker

Bot



Objects: Things (1)

Botnet



Cloud

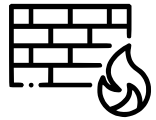
Computer

Cookie

Database

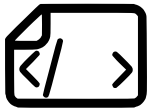
Memory

Firewall

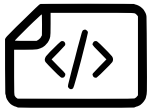


USB

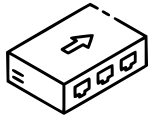
Custom File



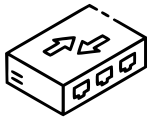
File



Hub



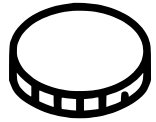
Switch



Router

Virus

Token



PII

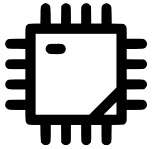
Private Key

Public Key

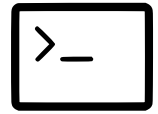
Generic Key

Password

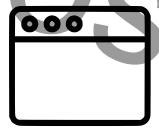
CPU



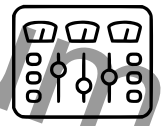
Shell



Webpage

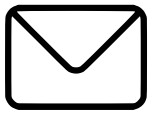


Industrial Control System

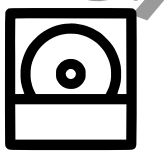


Objects: Things (2)

Message



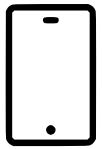
Memory



Port

Server

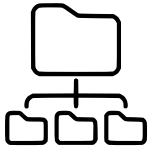
Smartphone



Software

Financial Information

Directory



Dark Web

Money

Annotations: Actions

DoS 

Injection 

Stop 

User Error 

Investigate 

Remove 

Annotations: States

Monitored

Cloaked

Buggy

Shielded

Corrupted

Ad Nauseum

Broken

Encrypted

Unencrypted

Hashed

Online

Offline

Vulnerable

Malicious

CIA Triangle

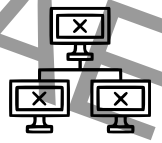
Disguised

Annotations: Components (1)

Trojan

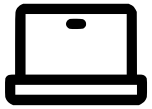
Worm

Botnet



Cloud

Computer

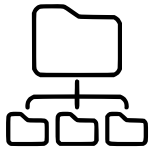


Cookie

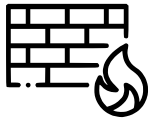
Database

Memory

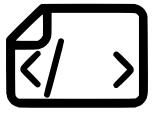
Directory



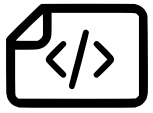
Firewall



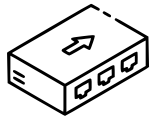
Custom File



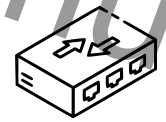
File



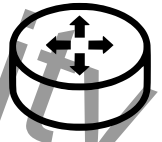
Hub



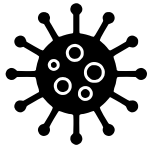
Switch



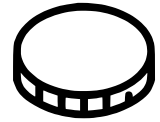
Router



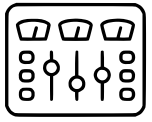
Virus



Token



Industrial Control System



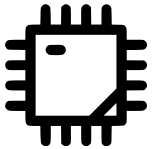
Private Key

Public Key

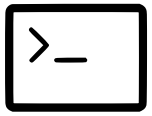
Generic Key

Password

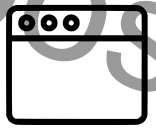
CPU



Shell



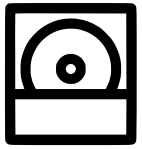
Webpage



Message

Annotations: Components (2)

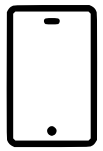
Memory



Port

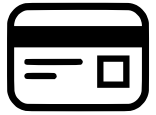
Server

Smartphone



Software

Financial Information



USB

PII

Dark Web

Money

2025 CAE Community Symposium

Practice Time

Trojan Horse Example Scenario

Objective:

CIA Violation:

Attack Type:

Steps:

1. …
2. …

Description:

An individual downloads a Minecraft plugin from an attacker's website disguised as a legitimate download website. The plugin contains hidden malicious code (i.e., a trojan) that installs a keylogger and reports all keystrokes back to the attacker who runs the disguised website, leading to compromised passwords and credentials.

Trojan Horse Example Scenario

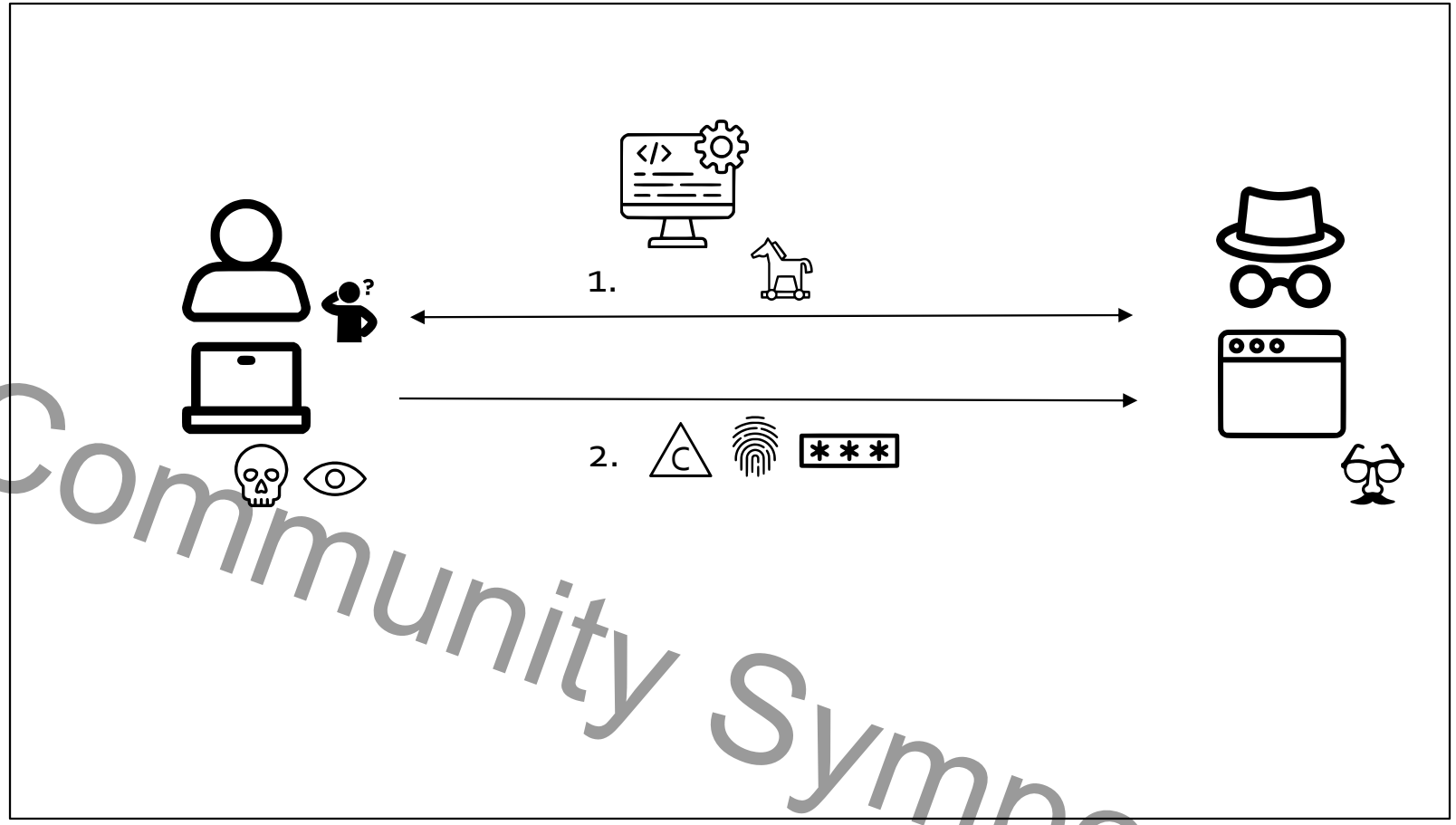
Objective: Steal Personal Information & Passwords

CIA Violation: Confidentiality

Attack Type: Trojan

Steps:

1. User downloads and installs Minecraft plugin from disguised site hosting malicious version with a keylogger
2. Keystroke data is sent to adversary from keylogger



Description:

An individual downloads a Minecraft plugin from an attacker's website disguised as a legitimate download website. The plugin contains hidden malicious code (i.e., a trojan) that installs a keylogger and reports all keystrokes back to the attacker who runs the disguised website, leading to compromised passwords and credentials.

Teaching with VAPOR

- Students “read” teacher-created diagrams to introduce CAPECs
  - Familiarize students to VAPOR
- Students practice diagramming a teacher-provided scenario
  - Check understanding of VAPOR
- Critique others’ diagrams
  - Reinforce understanding of VAPOR and ask questions based on diagrams
- Students create and diagram their own CAPEC scenarios
  - Develop adversarial mindset by creating & diagramming own scenarios
- Diagram a historical case study (e.g., Stuxnet, Mirai botnet)
  - Analyze complex case study with multiple stages

Lessons Learned

Strengths

- Process of creating is more useful than just "reading" them
- Shows the context of attacks
- Visual representation of student understanding
- Current Gen-AI can't diagram using this system

Limitations

- Time commitment to understand initial system and rules
- Using PowerPoint can be frustrating when building diagrams
- There are multiple right answers to a problem, so grading can be hard to approach systematically

Based on interviews, observations, assignment descriptions, and teacher feedback in 3 semesters of Adversarial Thinking class

2025 CAE Community Symposium

Questions & Answers