CSCI 476: Computer Security

Threat Modeling

Reese Pearsall

Fall 2024

*all images are stolen from the internet

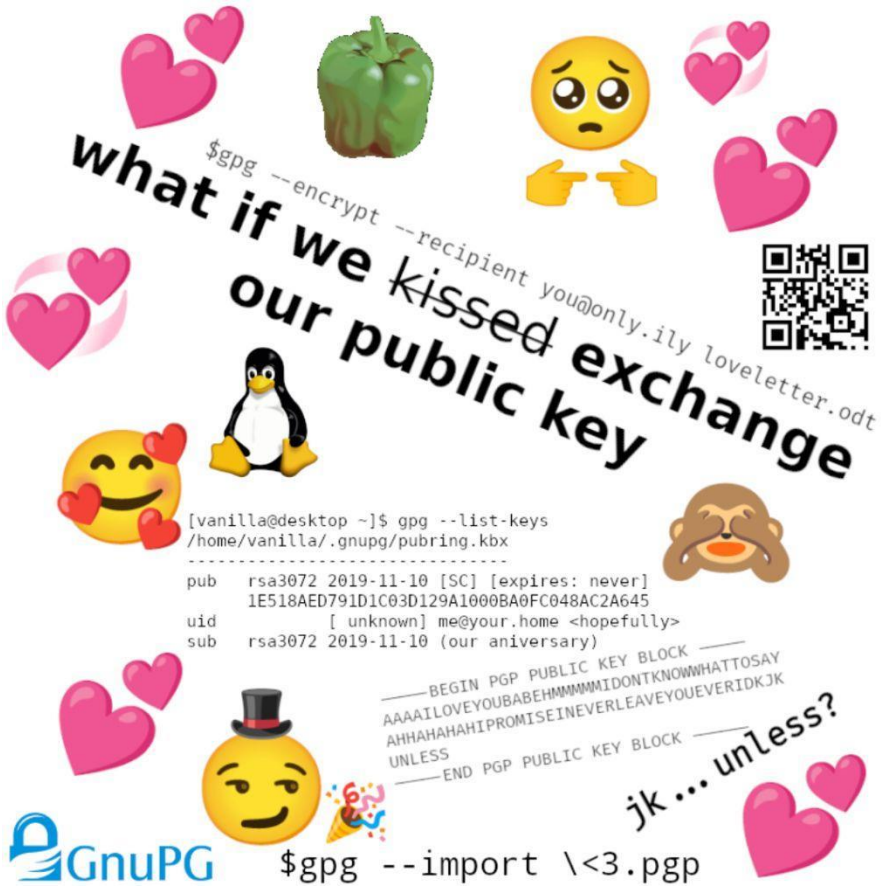
Announcements

Lab 9 due Sunday **12/8**

Please fill out the course evaluation (Extra Credit)

<u>Final Exam</u>
Tuesday December 10th 2:00 – 3:50 in Romney 315
You are allowed one notesheet. Study guide posted soon

Please be there



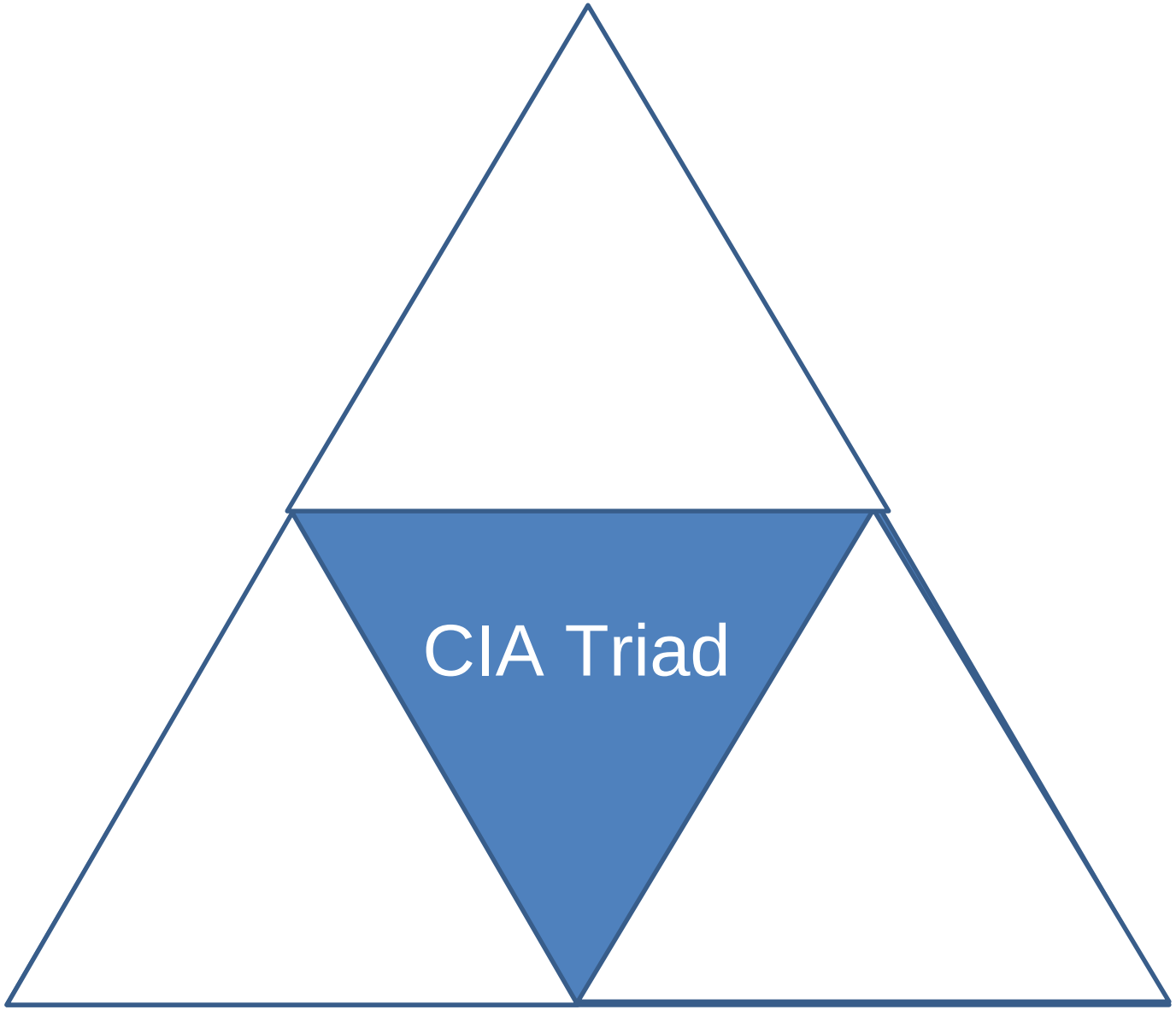
If you are taking the exam at the testing center, make sure you schedule it before friday

Please look at your grades and let me know if you are missing anything


EXTRA CREDIT

Security Basics

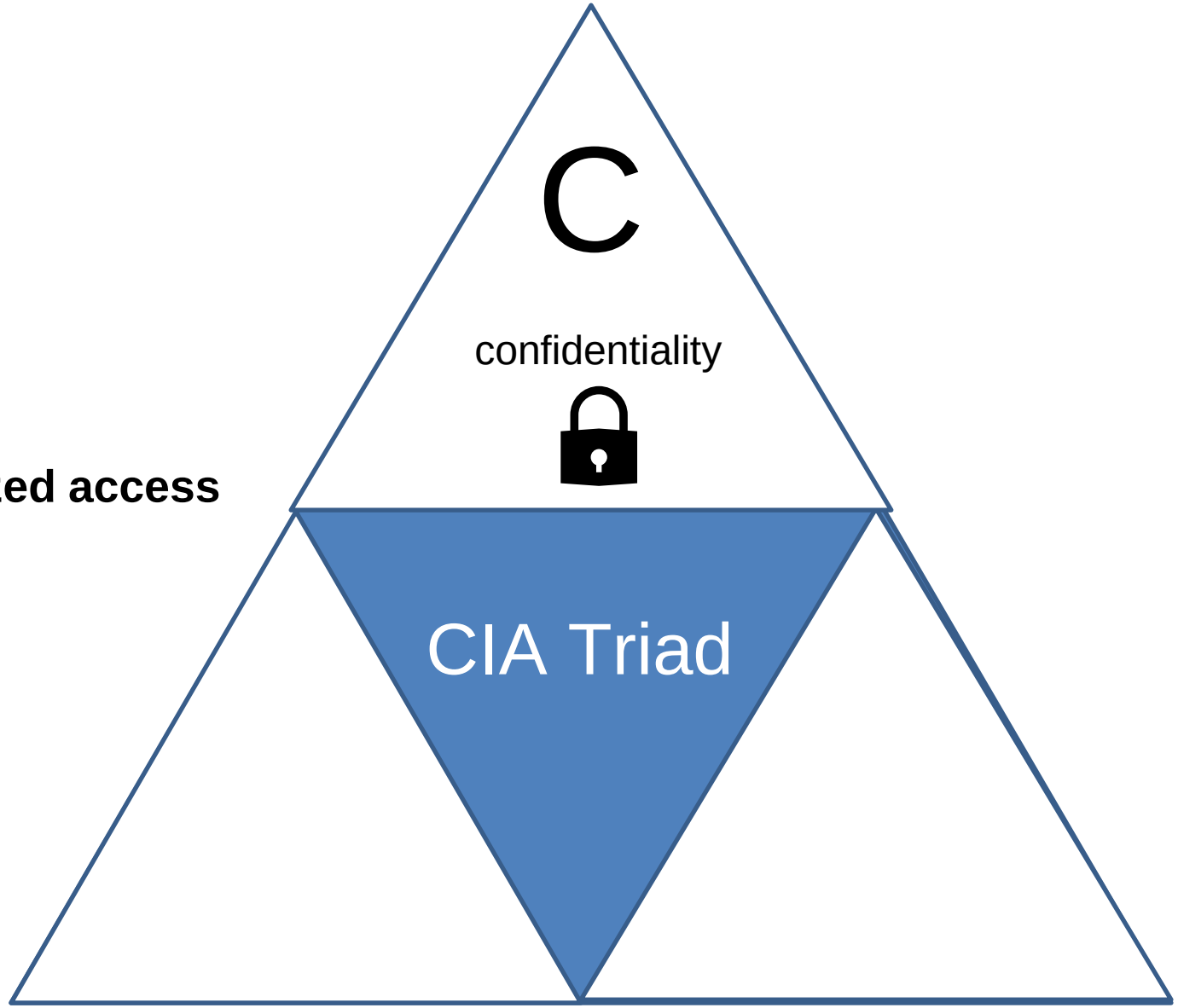
The **CIA Triad** is a widely accepted model for evaluating the security of a system. Consists of three important principles



Security Basics

The **CIA Triad** is a widely accepted model for evaluating the security of a system. Consists of three important principles

Confidentiality- protection from **unauthorized access**

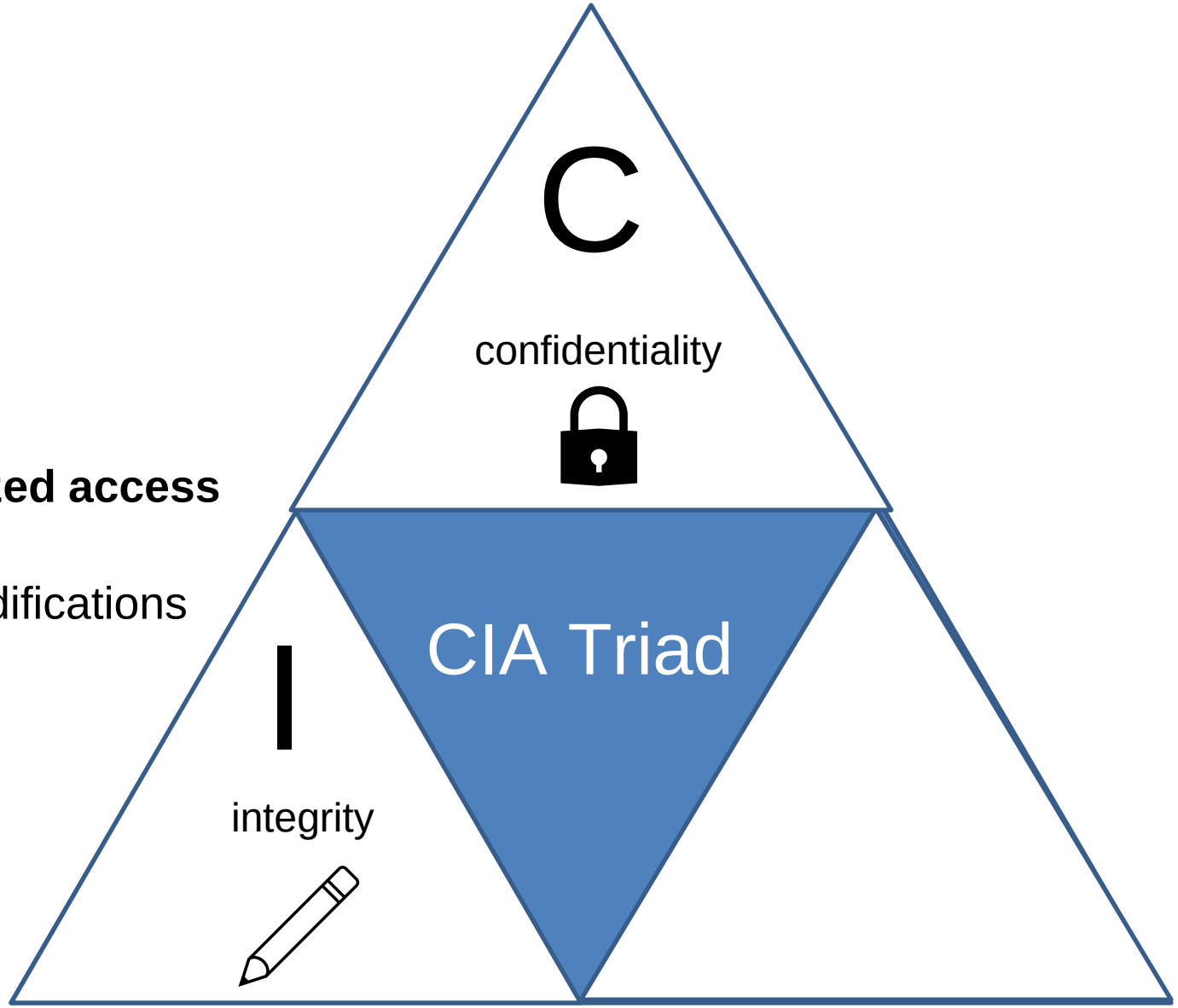


Security Basics

The **CIA Triad** is a widely accepted model for evaluating the security of a system. Consists of three important principles

Confidentiality- protection from **unauthorized access**

Integrity- protection from unauthorized modifications



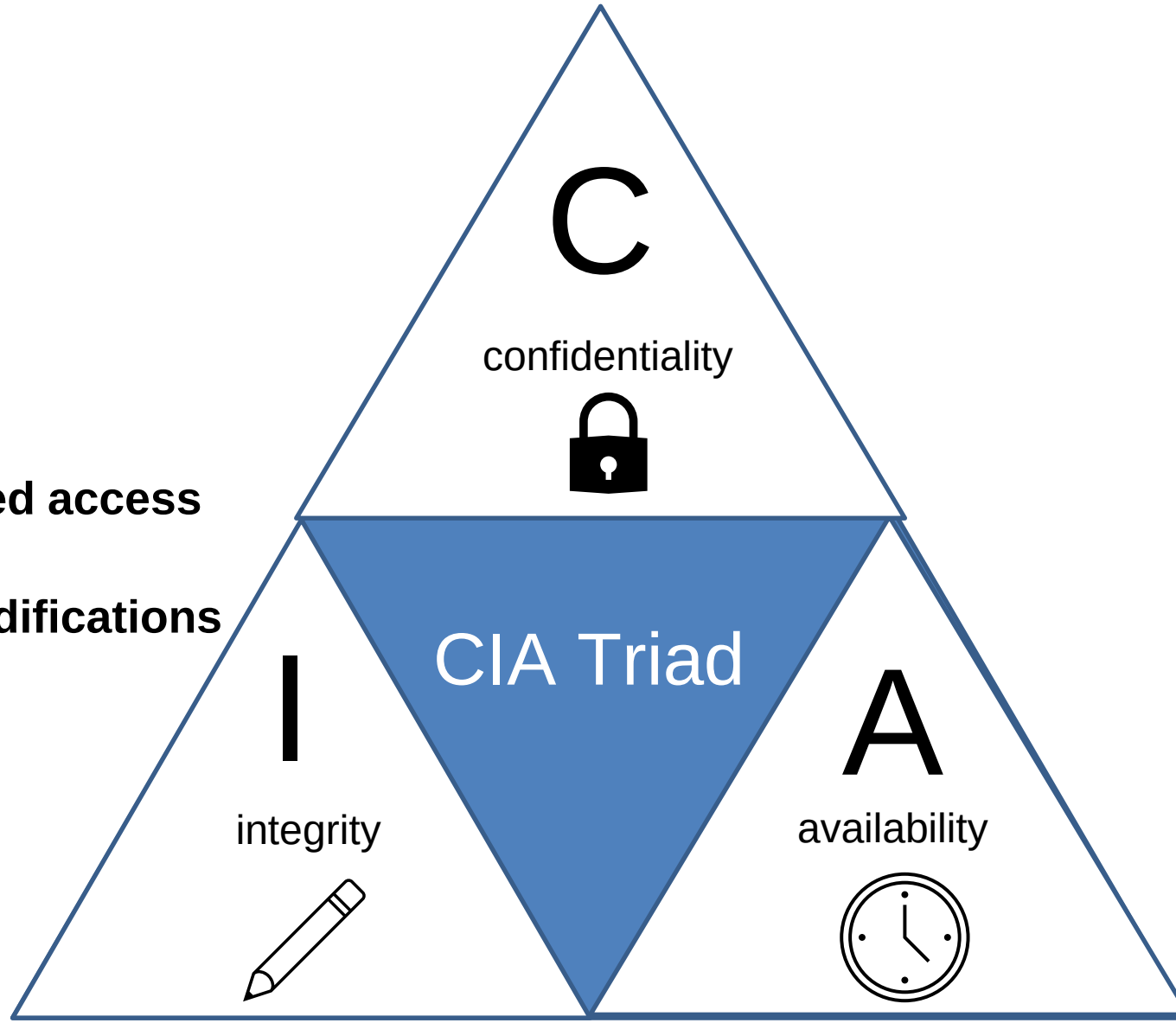
Security Basics

The **CIA Triad** is a widely accepted model for evaluating the security of a system. Consists of three important principles

Confidentiality- protection from **unauthorized access**

Integrity- protection from **unauthorized modifications**

Availability- protection from **interruption**



Common Threats & Attack Vectors

Denial of Service (DoS / DDos)- attack with intent to shut down a machine or network

- Violates the **availability** property

Common Threats & Attack Vectors

Denial of Service (DoS / DDos)- attack with intent to shut down a machine or network

- Violates the **availability** property

Information Leakage / Data Corruption- unauthorized or accidental reveal of sensitive information

- Violates the **confidentiality** property
- Violates the **integrity** property

Common Threats & Attack Vectors

Denial of Service (DoS / DDos)- attack with intent to shut down a machine or network

- Violates the **availability** property

Information Leakage / Data Corruption- unauthorized or accidental reveal of sensitive information

- Violates the **confidentiality** property
- Violates the **integrity** property

Privilege Escalation- gaining illicit permissions beyond what is intended for that user

- Violates the **confidentiality** property
- Violates the **integrity** property

Defense Mechanisms

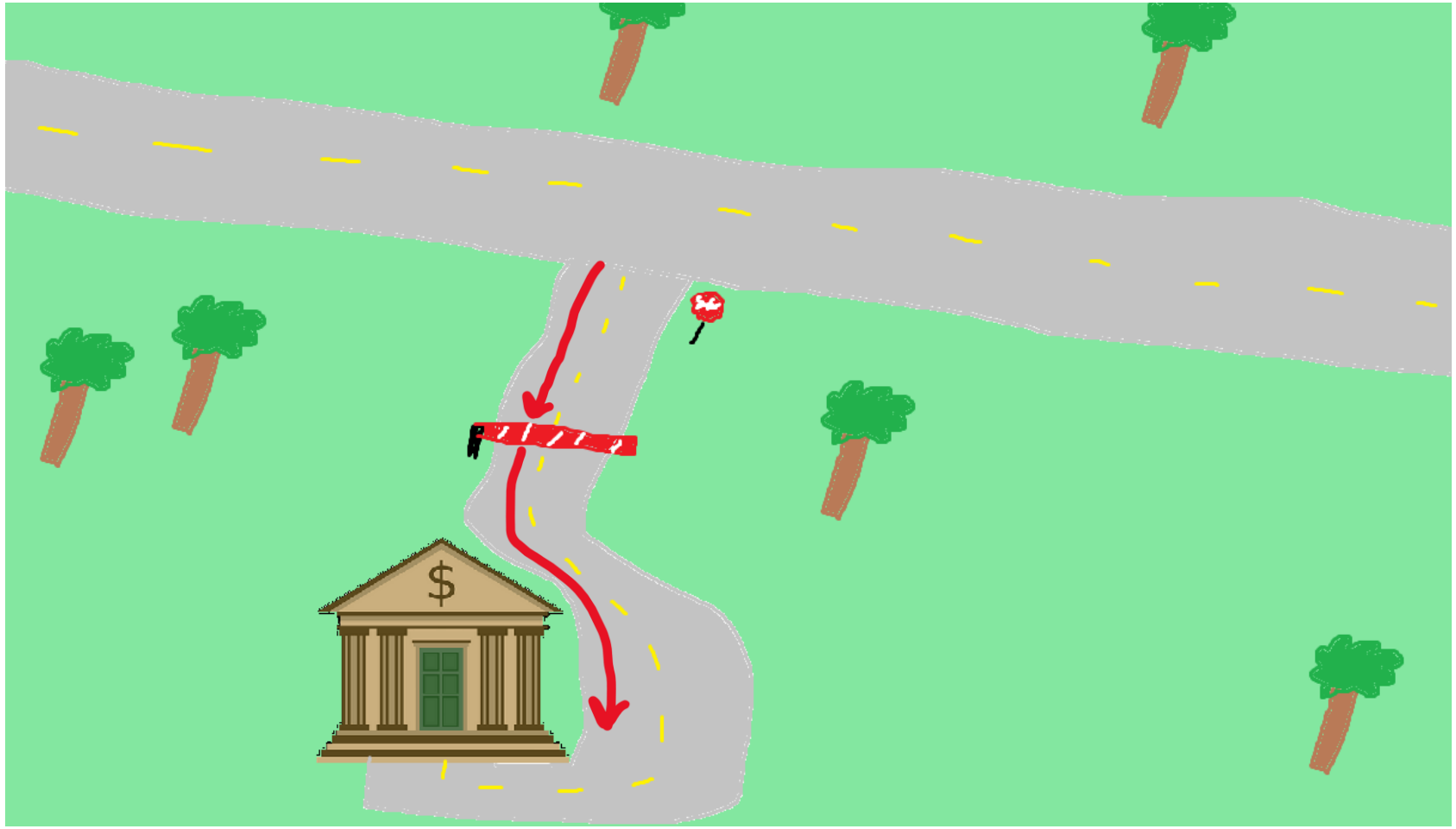
- Countermeasures (ASLR, SYN Cookies, etc)
- Software testing
- Formal verification
- Refactoring software and safe coding practices

Threat Modeling

NEED: a consistent and structured approach for defense and assessing risk

Assessing Risk

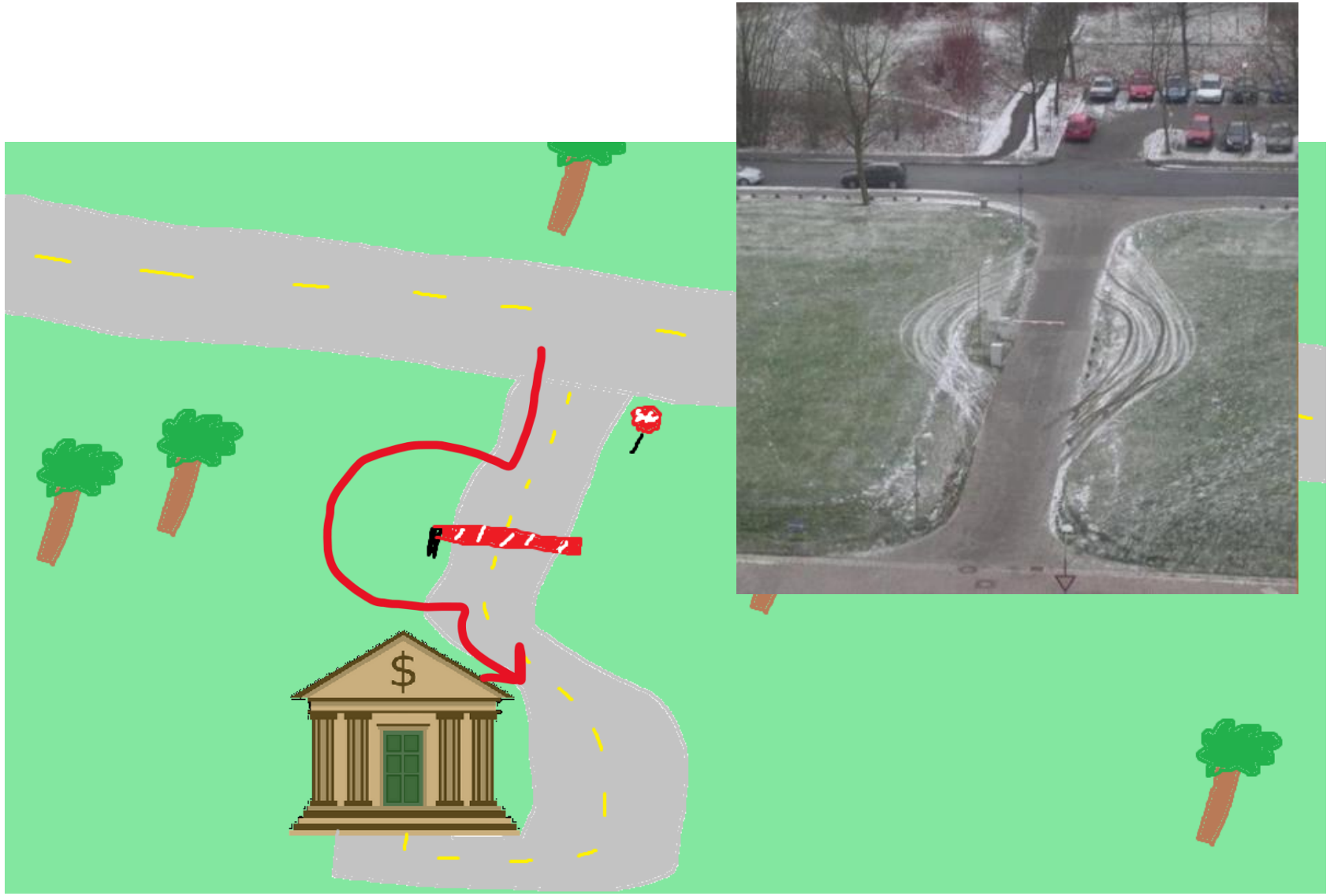
We expect users to interact with our system in a certain way



Assessing Risk

We expect users to interact with our system in a certain way

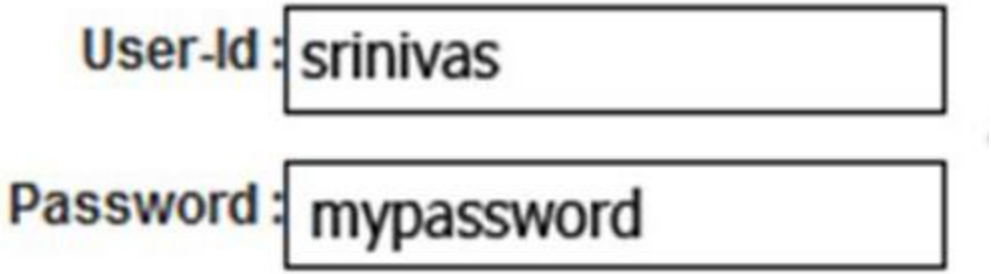
When someone interacts with our system in a way that we did not intend… it could have harmful consequences



Assessing Risk

We expect users to interact with our system in a certain way

When someone interacts with our system in a way that we did not intend… it could have harmful consequences



We might expect a user to input a valid username and password when they attempt to log in

Assessing Risk

We expect users to interact with our system in a certain way

When someone interacts with our system in a way that we did not intend… it could have harmful consequences

User-Id : srinivas

Password : mypassword

We might expect a user to input a valid username and password when they attempt to log in

What if they did something…….. weird?

User-Id : ' OR 1= 1; /*

Password : */--

Assessing Risk

We expect users to interact with our system in a certain way

When someone interacts with our system in a way that we did not intend… it could have harmful consequences

User-Id : srinivas

Password : mypassword

We might expect a user to input a valid username and password when they attempt to log in

What if they did something…….. weird?

User-Id : ' OR 1= 1; /*

Password : */--

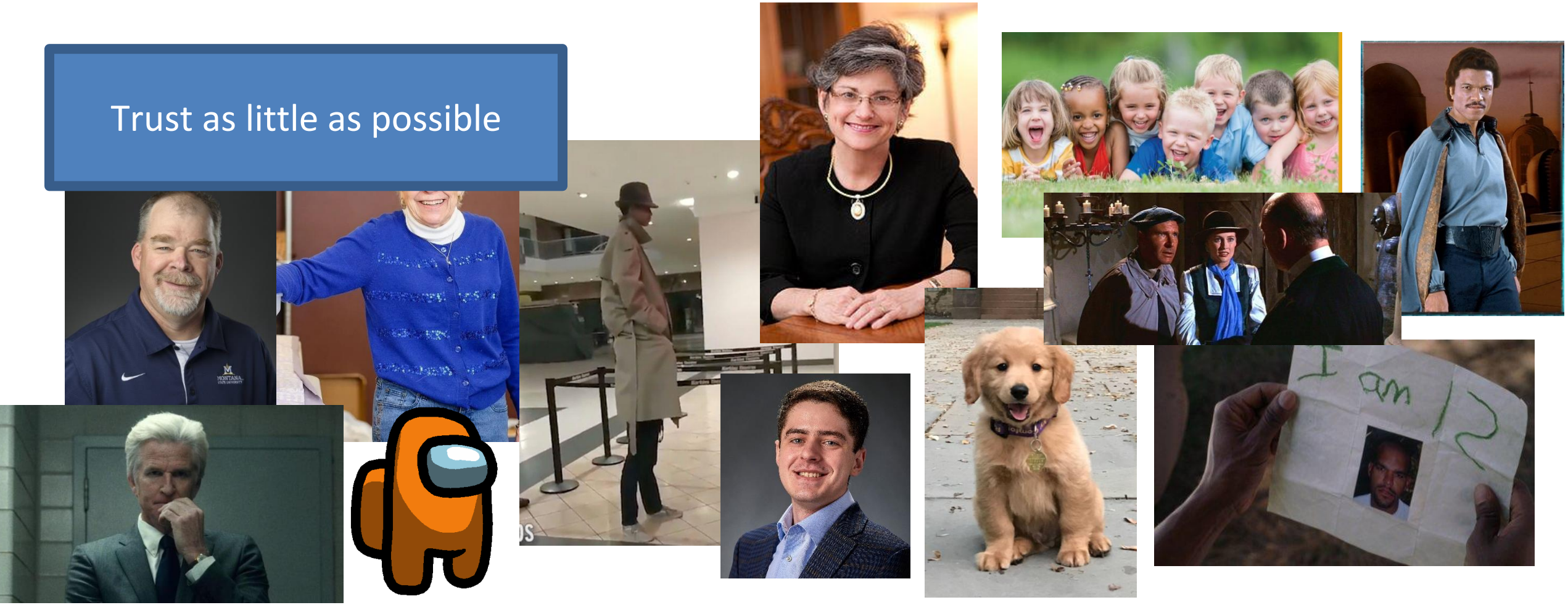
LOGIN SUCCESS

Who do we trust?

Are they honest? Are they reliable? Are they dependable? What are their intentions?

Who do we trust?

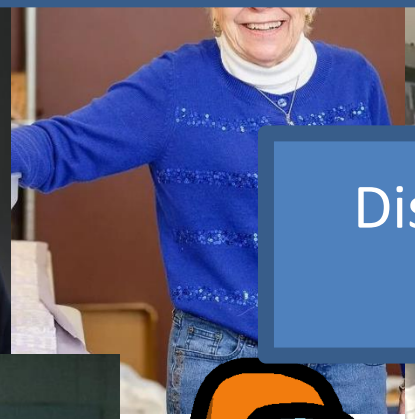
Trust as little as possible

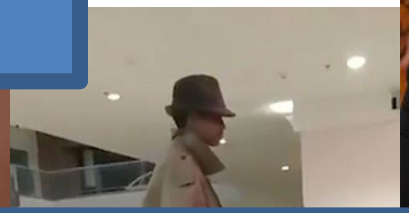


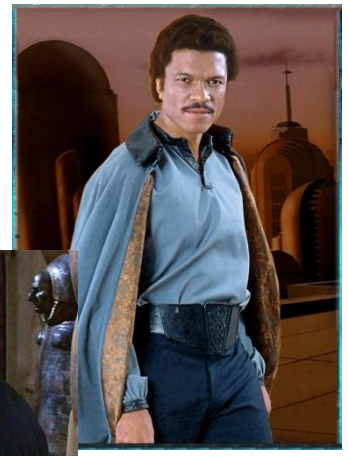
Are they honest? Are they reliable? Are they dependable? What are their intentions?

Who do we trust?

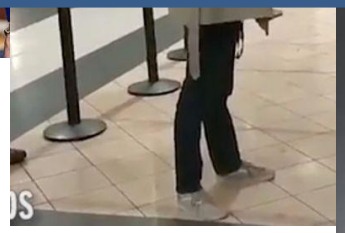
Trust as little as possible

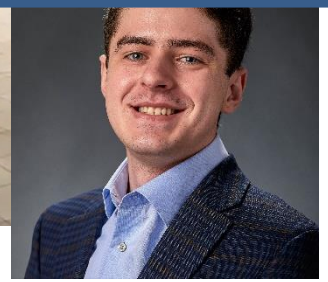


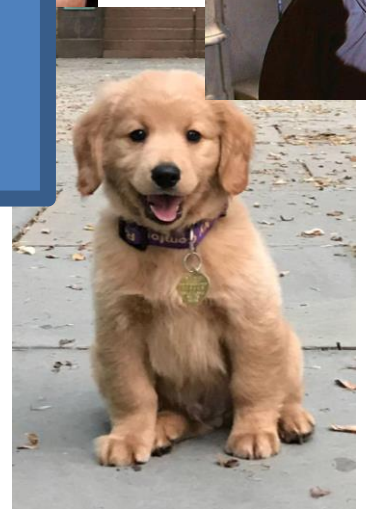


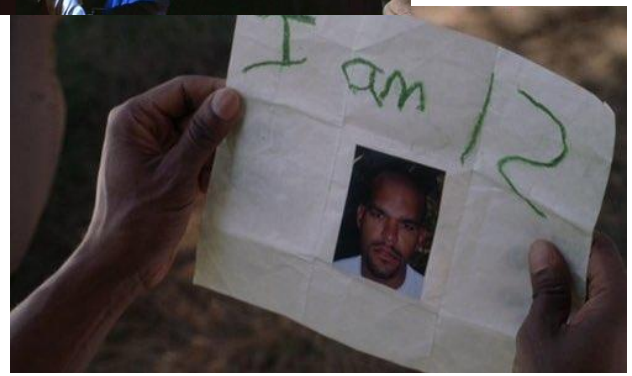


Distrust proportionally to level of risk









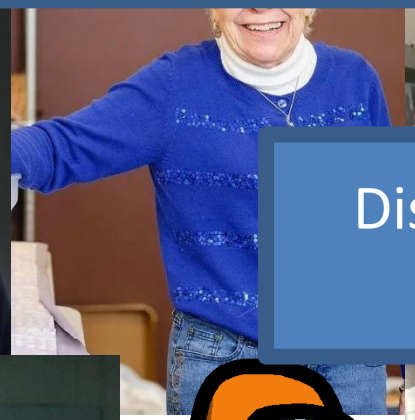
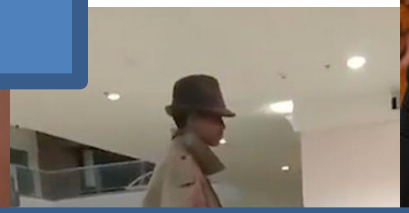
Are they honest? Are they reliable? Are they dependable? What are their intentions?

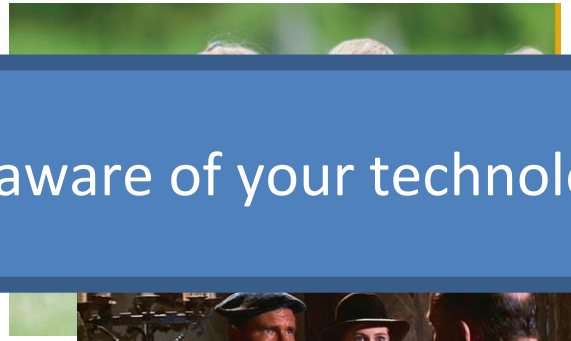
Who do we trust?

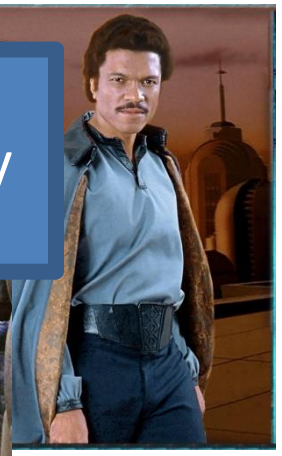
Trust as little as possible

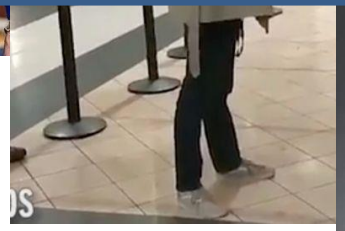
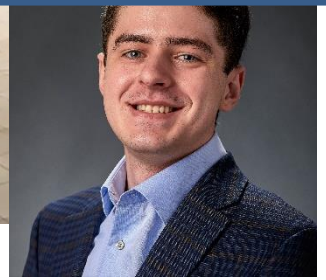
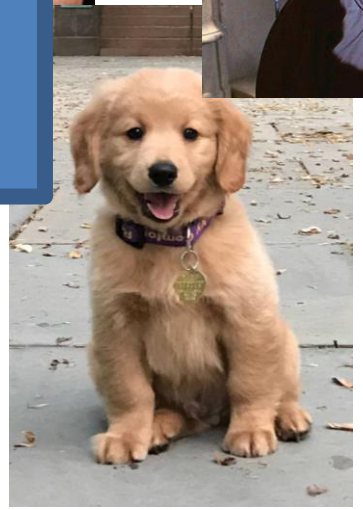
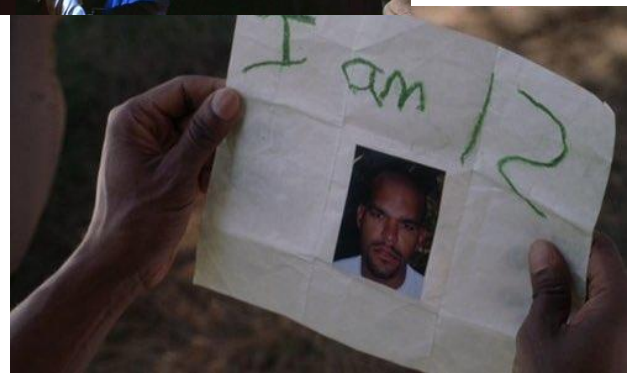
Be aware of your technology

Distrust proportionally to level of risk

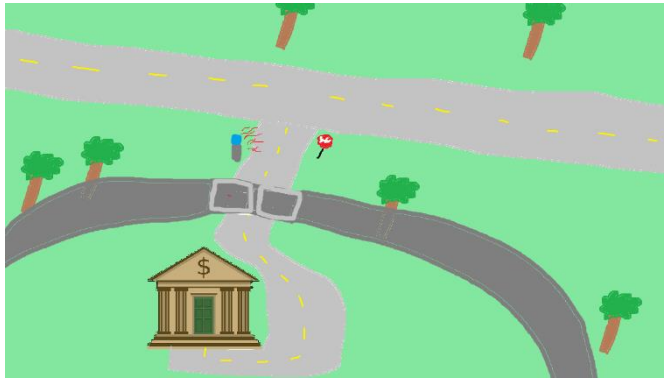




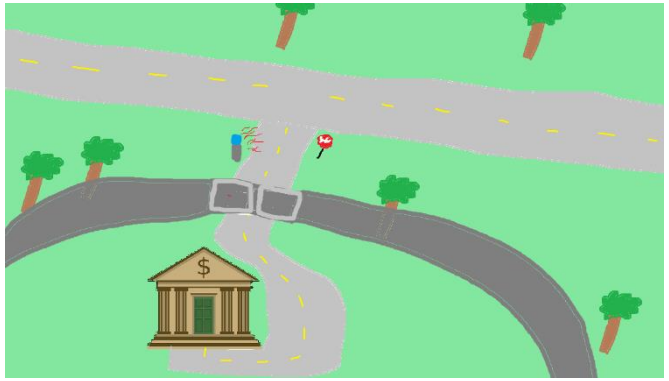
Are they honest? Are they reliable? Are they dependable? What are their intentions?

Perfect security is impossible



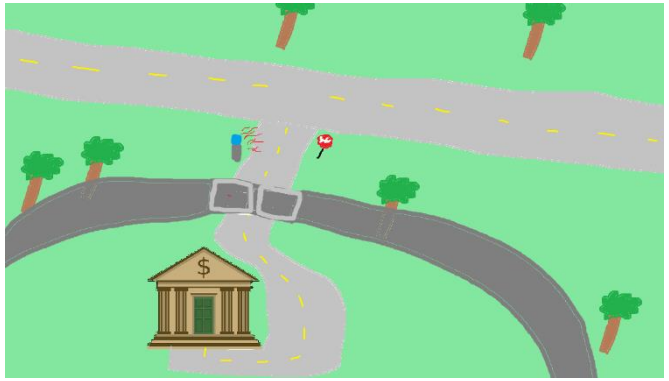
Perfect security is impossible

- New **assets**



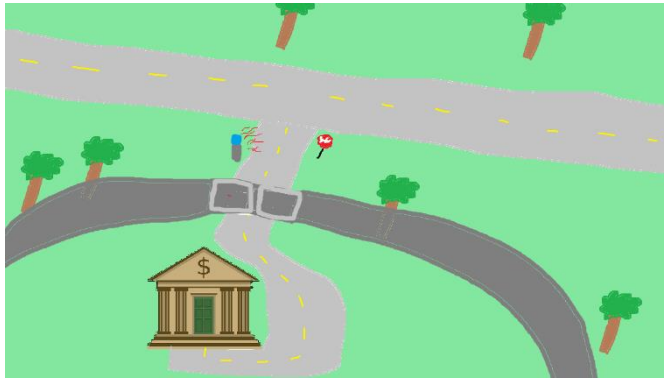
Perfect security is impossible

- New **assets**
- New **threats**



Perfect security is impossible

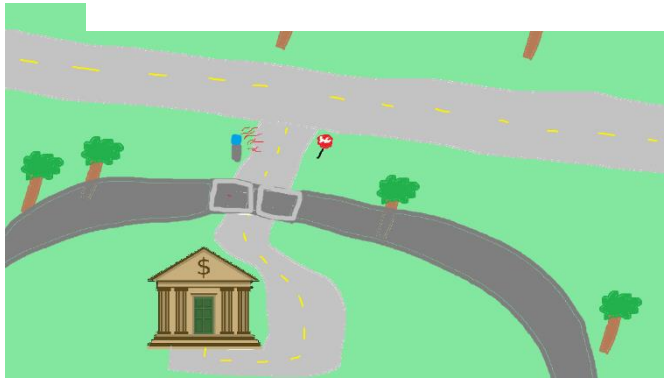
- New **assets**
- New **threats**
- New **capabilities**



Perfect security is impossible

- New **assets**
- New **threats**
- New **capabilities**
- New **technology**

Apache LOG4J 2 ™

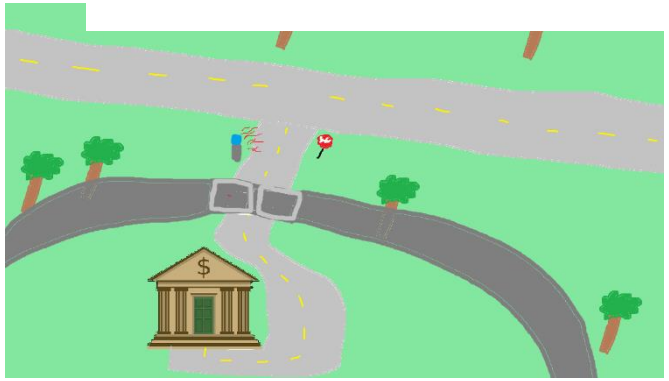


Perfect security is impossible

- New **assets**
- New **threats**
- New **capabilities**
- New **technology**

My goal is to teach you important cybersecurity principles that are universal across any system

Apache LOG4J™



NEWS 25 OCT 2023

Winter Vivern: Zero-Day XSS Exploit Targets Roundcube Servers

Heap-based Buffer Overflow Flaw in cURL Library Using SOCKS5 Proxy

By Eswar - October 12, 2023

AIOS WordPress Plugin Faces Backlash for Storing User Passwords in Plaintext

Jul 14, 2023 Newsroom Password Security / WordPress

Cloudflare website downed by DDoS attack claimed by Anonymous Sudan

Threat Modeling

You develop a threat model by focusing on five key questions

1. What are you building?
2. What are the assets?
3. What can go wrong? What are the threats?
4. What mechanisms can we implement to prevent things from going wrong?
5. Did you do a decent job of analysis?

Threat Modeling

Brainstorming

1. **Free-form brainstorming-** gather around a whiteboard; enumerate threats/possible defenses
2. **Scenario Analysis-** Propose a scenario and ask “what might go wrong?”
3. **Pre-Mortem**- Assuming a failure or compromise, what do you do next?
4. **Movie plotting** – Pick outrageous ideas; what happens next?
5. **Literature review-** study systems that are similar to yours

Threat Modeling Practice

1. **Free-form brainstorming-** gather around a whiteboard; enumerate threats/possible defenses
2. **Scenario Analysis-** Propose a scenario and ask “what might go wrong?”
3. **Pre-Mortem**- Assuming a failure or compromise, what do you do next?
4. **Movie plotting** – Pick outrageous ideas; what happens next?
5. **Literature review-** study systems that are similar to yours

Let's develop a threat model

You are at a bar, and you hand your phone to a cute person …

Threat Modeling Practice

1. **Free-form brainstorming-** gather around a whiteboard; enumerate threats/possible defenses
2. **Scenario Analysis-** Propose a scenario and ask “what might go wrong?”
3. **Pre-Mortem**- Assuming a failure or compromise, what do you do next?
4. **Movie plotting** – Pick outrageous ideas; what happens next?
5. **Literature review-** study systems that are similar to yours

Let's develop a threat model

You are at a bar, and you hand your phone to a cute person …

1. What are you building?
2. What are the assets?
3. What can go wrong? What are the threats?
4. What mechanisms can we implement to prevent things from going wrong?
5. Did you do a decent job of analysis?

Structured Approaches

WE NEED STRUCTURE

- Attack Lists & Libraries (ie. Common and Current vulnerabilities)

There is no “right” choice

Structured Approaches

On the final lab, you will need to use the knowledge you've learned in this class to develop a threat model for some kind of software system

- Attack Lists & Libraries (ie. Common and Current vulnerabilities)

There is no "right" choice

Structured Approaches

- **Asset-centric**: focus on things of value: things attack want; things you want to protect
- **Attacker-centric**: focus on attackers/archetypes/personas and their capabilities
- **Software-centric**: focus of SW; most SW is backed by structured models (CFG, State diagrams, etc)

Methodologies

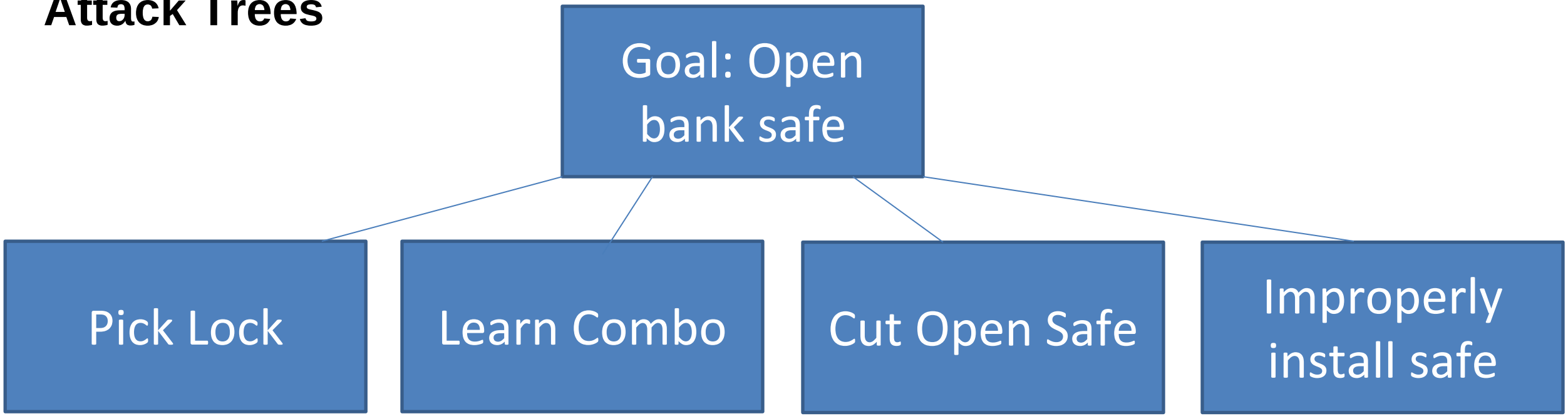
- STRIDE
  - **S**poofing, **T**ampering, **R**epudiation, **I**nfo Disclosure, **D**enial of Service, **E**levation of Privilege
    (https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats)
- Attack Trees
- Attack Lists & Libraries (ie. Common and Current vulnerabilities)

There is no “right” choice

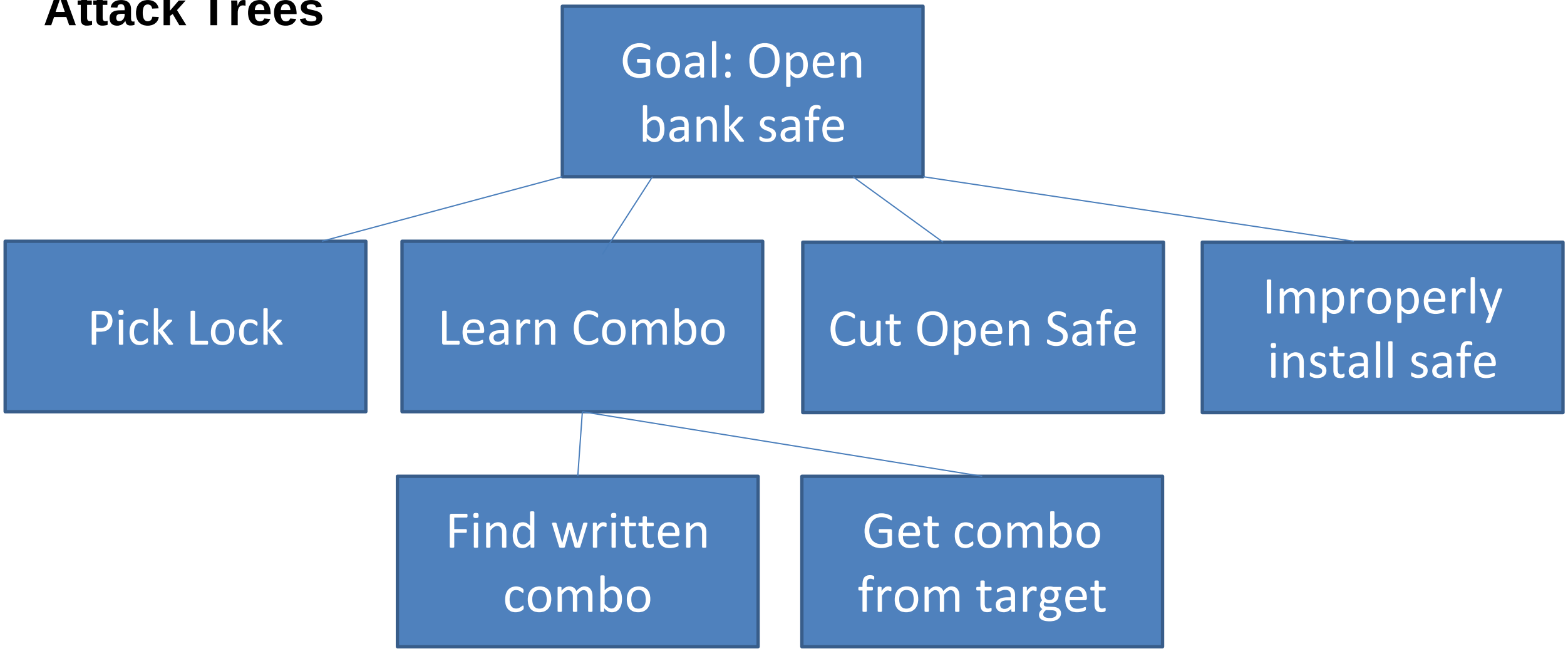
Attack Trees

Goal: Open bank safe

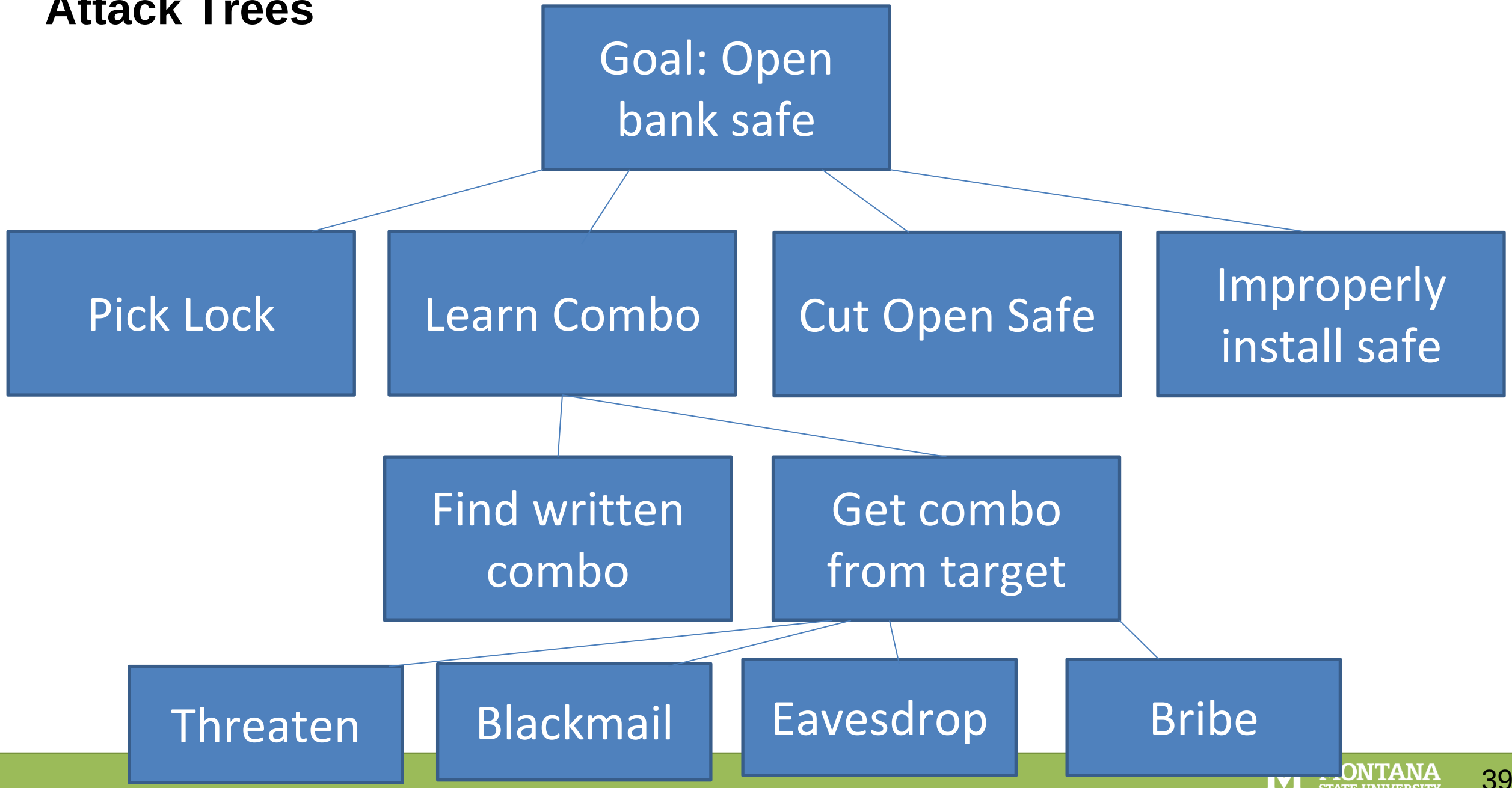
Attack Trees



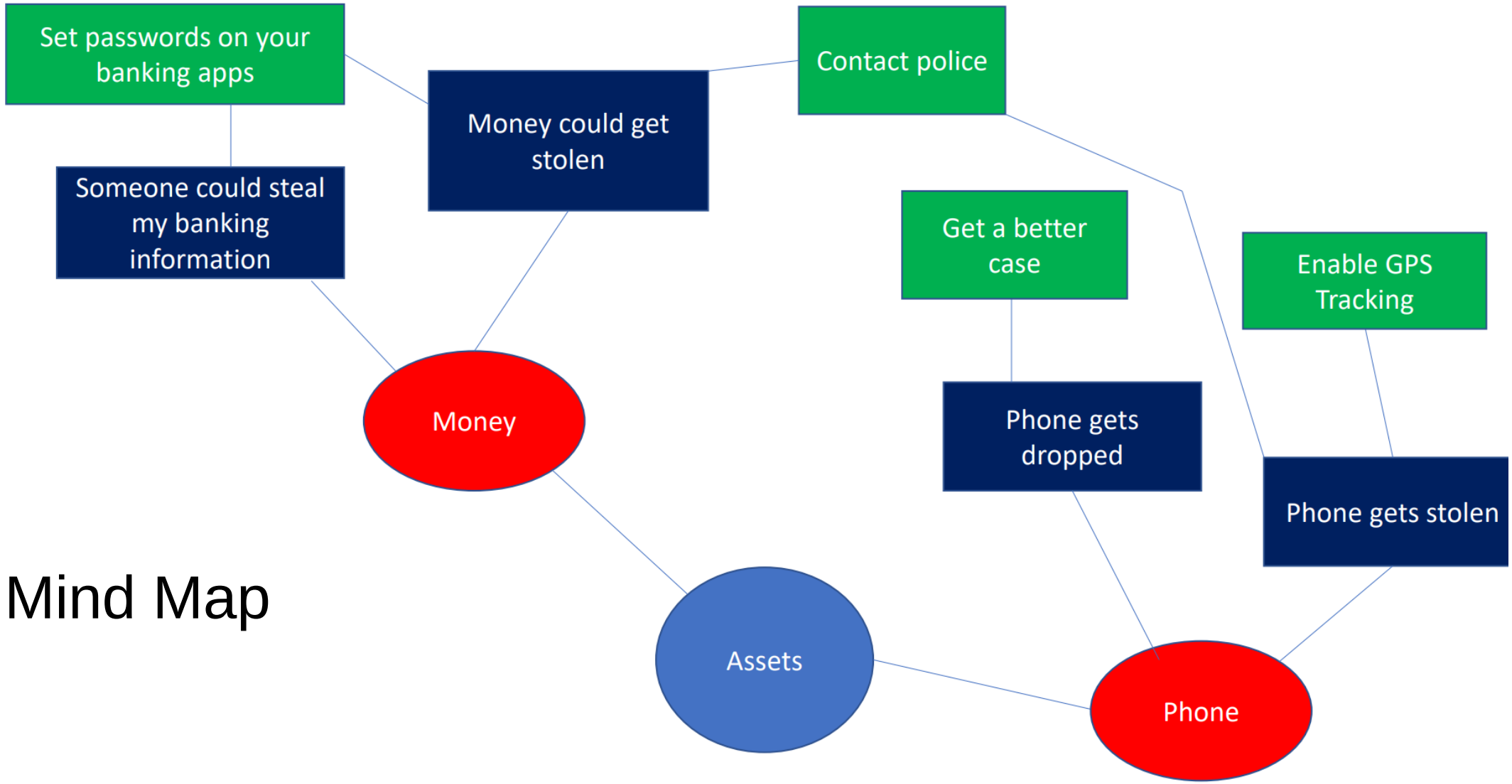
Attack Trees

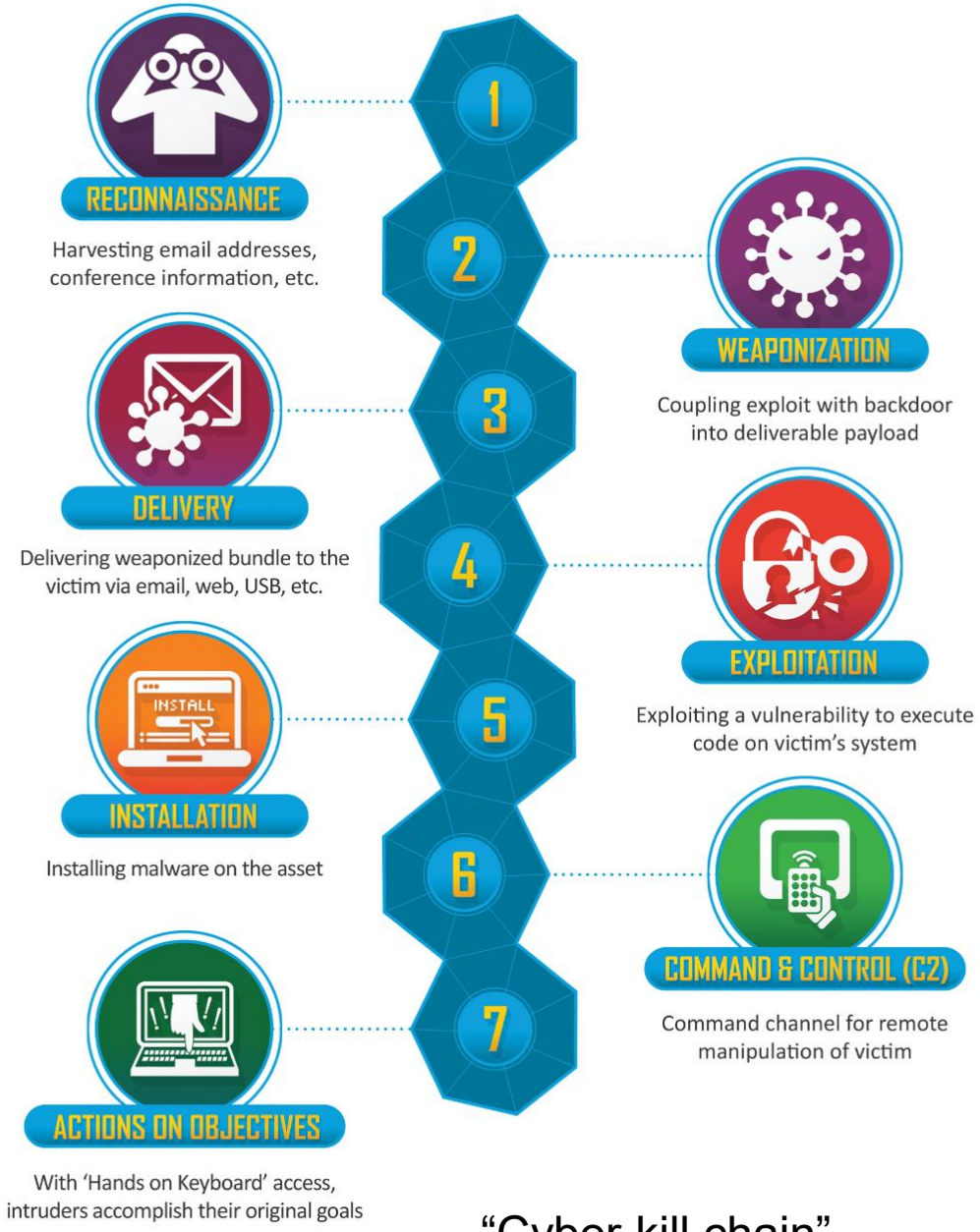


Attack Trees



Mind Map


Set passwords on your banking apps
Money could get stolen
Contact police
Someone could steal my banking information
Get a better case
Enable GPS Tracking
Money
Phone gets dropped
Phone gets stolen
Assets
Phone

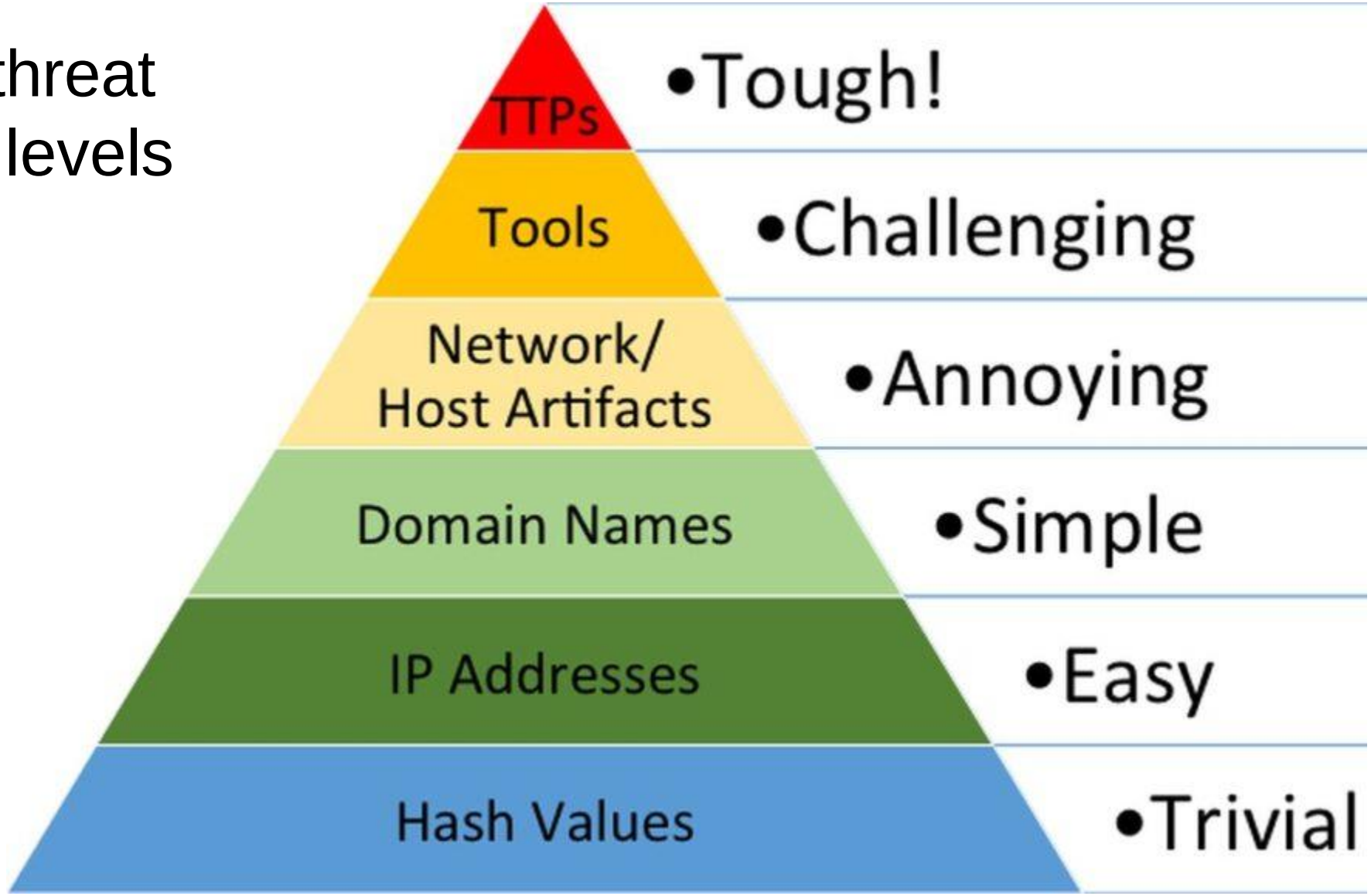


"Cyber kill chain"

Be aware of the steps taken by a cybercriminal to conduct some cyber attack

Responding to a threat can have varying levels of difficulty

Indicators of compromise (IOCs) refer to data that indicates a system may have been infiltrated by a cyber threat. They provide cybersecurity teams with crucial knowledge after a data breach or another breach in security.



"Pyramid of Pain"

Legitimate organizations must meet **compliance** standards if they want to do business. This includes things such as handling transactions securely, encrypting user data, no plaintext passwords, etc

These rules are structured as a compliance framework, which is a structures set of guidelines and best practices that details a company's processes for meeting regulatory requirements

STIG - 230503

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

STIG - 230534

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

STIG - 217976

*The audit system must be configured to audit all use of **setuid** and setgid programs.*

STIG - 217976

*The Ubuntu operating system must implement **address space layout randomization** to protect its memory from unauthorized code execution.*

.

STIG - 230231

RHEL 8 must encrypt all stored passwords with a FIPS 140-2 approved **cryptographic hashing** algorithm.

SHA-256, SHA-512, etc