

# CSCI 476: Computer Security

Lecture 4: Introduction to Security + Threat Modeling

Reese Pearsall  
Fall 2022

# Announcements

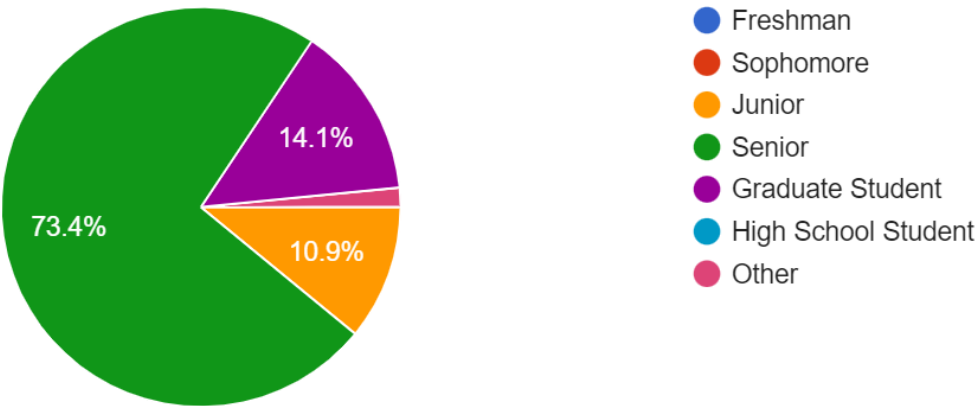
TA

- **Karishma Rahman**
- karishma.rahman.bd@gmail.com
- Office Hours: Tuesdays 1:00 pm to 3:00 pm
- Location: Barnard 259

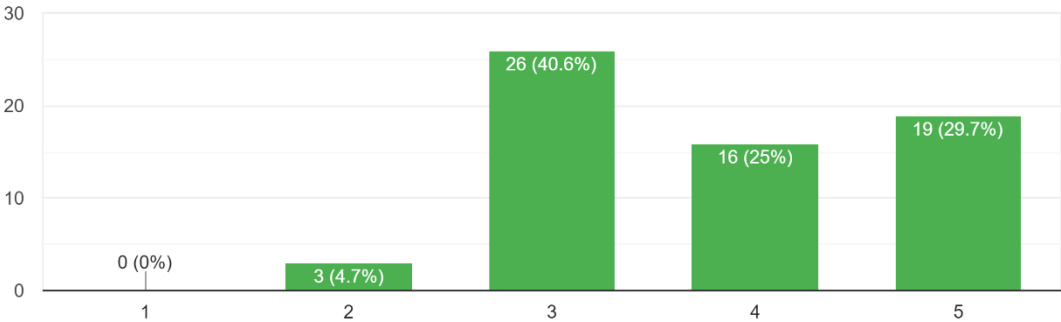
Lab 1 Due Thursday 9/15 @ 11:59 PM

You have one late pass for the semester

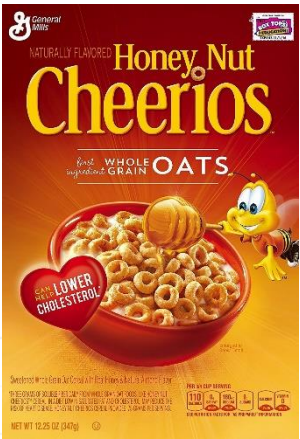
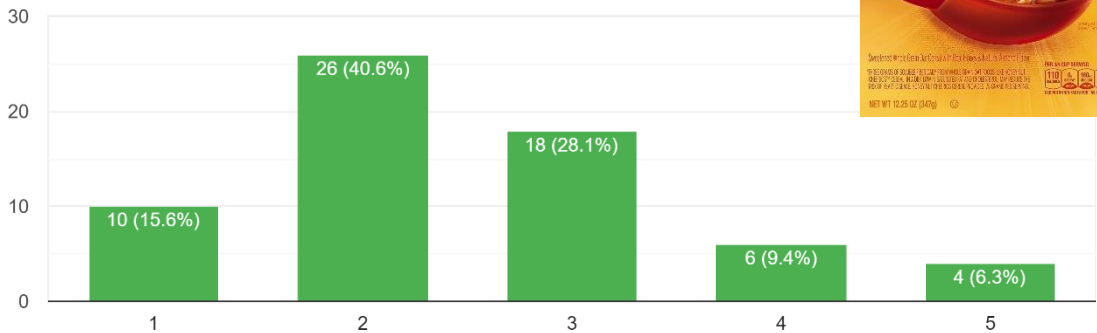
# From the questionnaire...



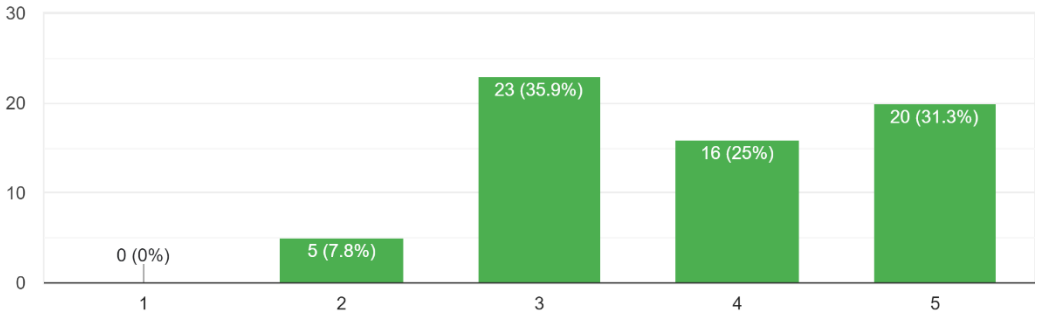
How comfortable are you C?  
64 responses



How comfortable are you with reading assembly code?  
64 responses



How comfortable are you with using the Linux command line? (cd, ls, mkdir, grep, chmod, etc)  
64 responses



What is security?

(What is security **not**?)

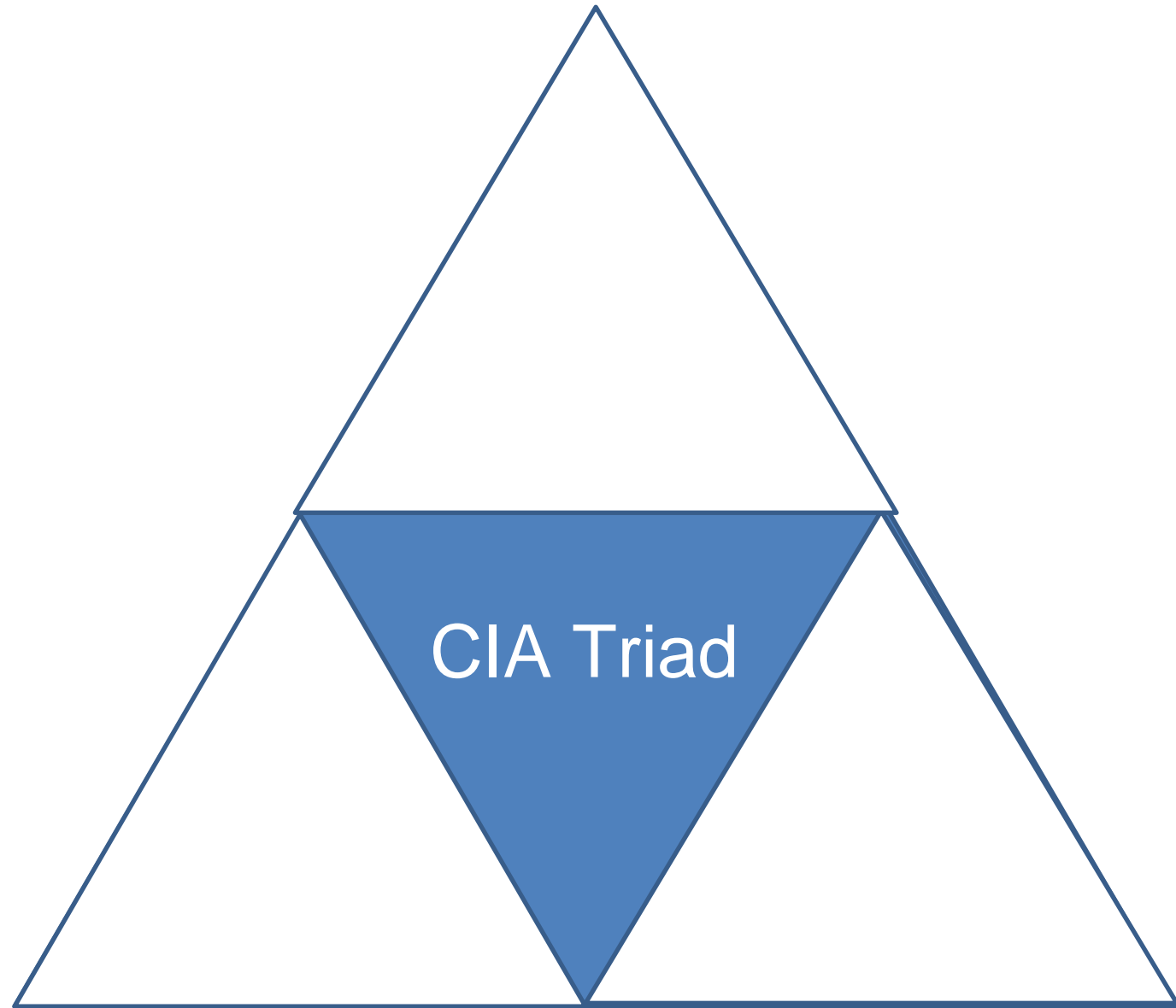
# Why is it important?

Popular examples? Examples you've encountered?

# What can we do about security issues?

# Security Basics

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

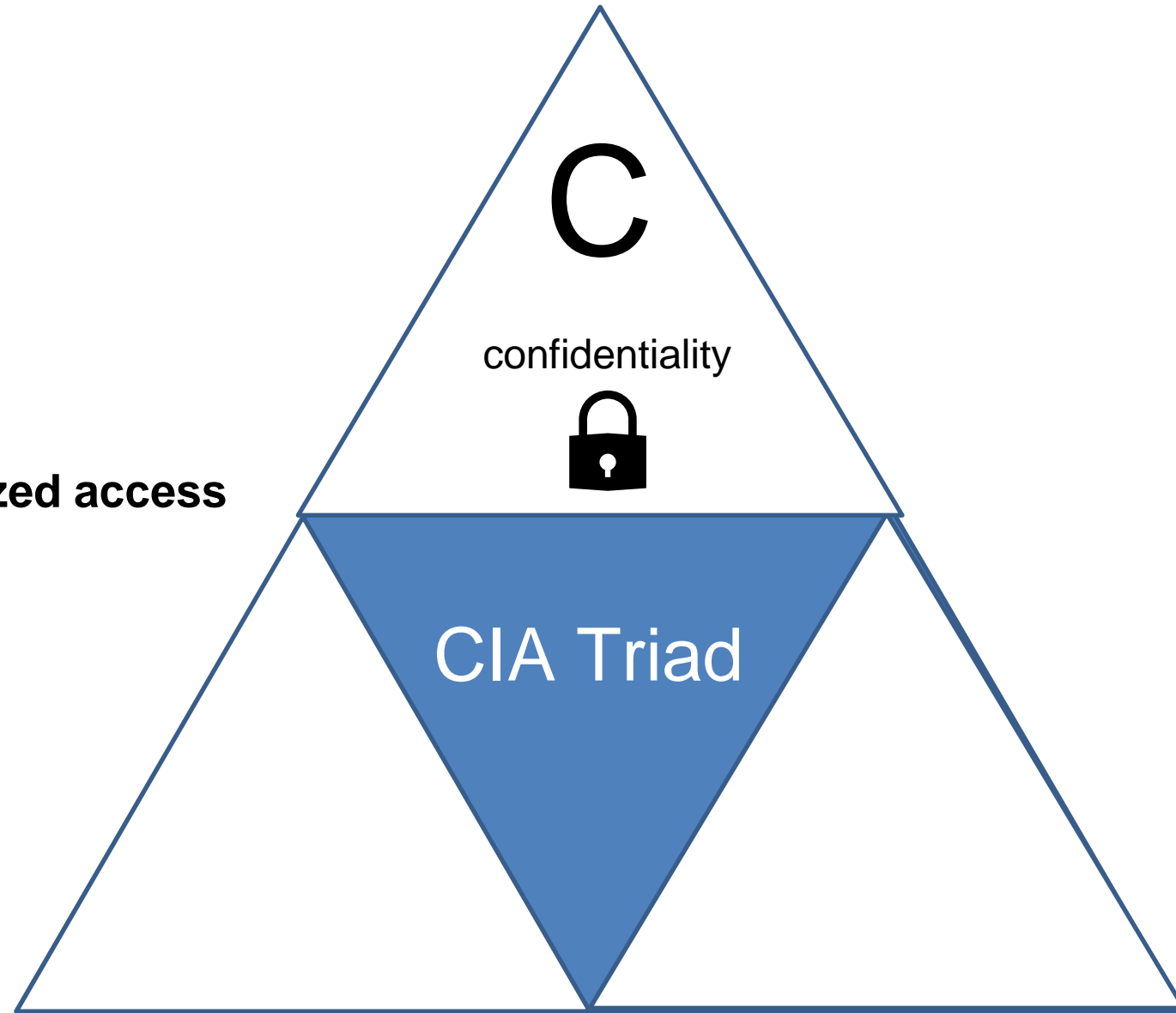




# Security Basics

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**

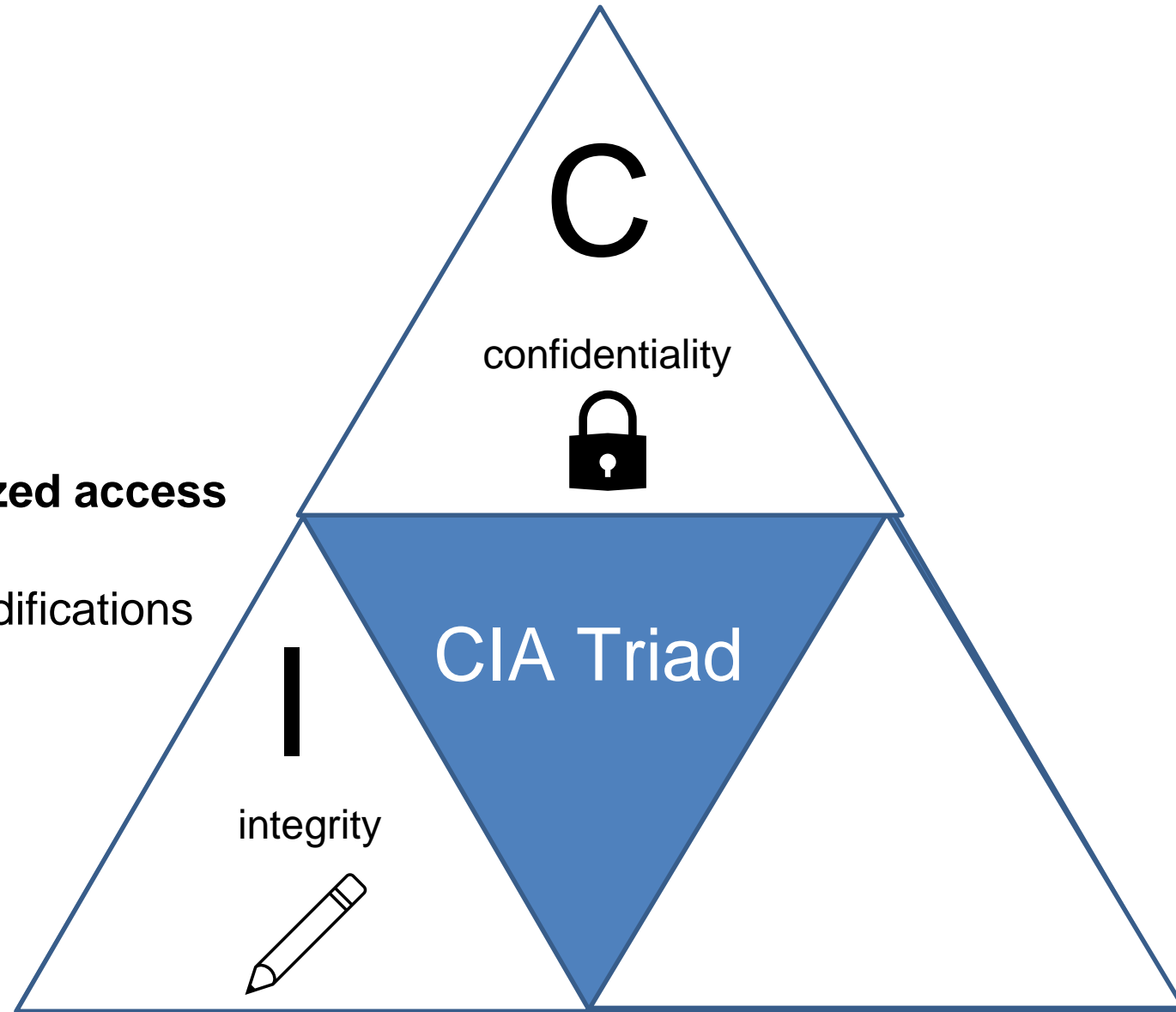


# Security Basics

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



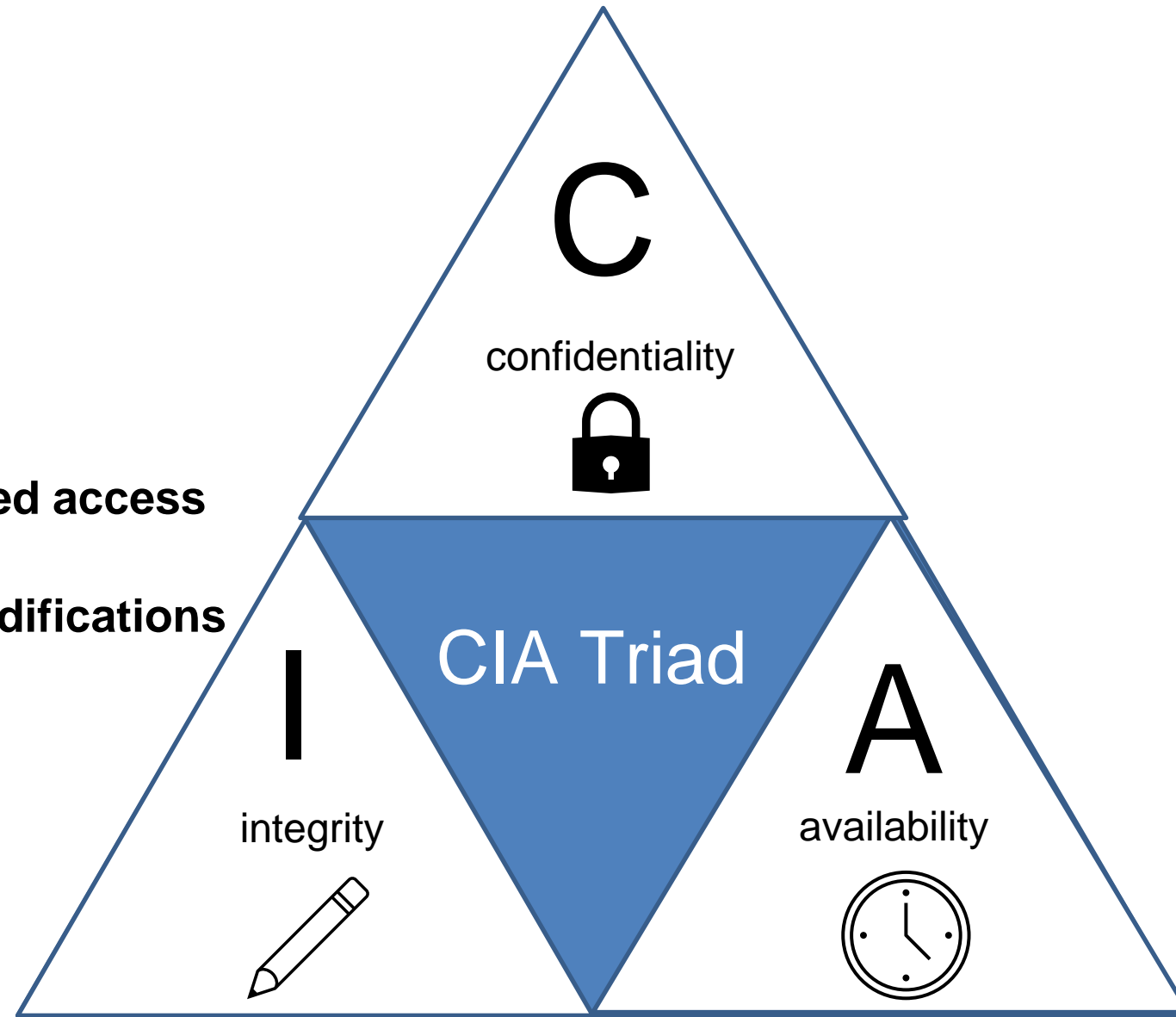
# Security Basics

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

- Formal verification
- Software testing
- Refactoring software and safe coding practices
- Built-in mitigations



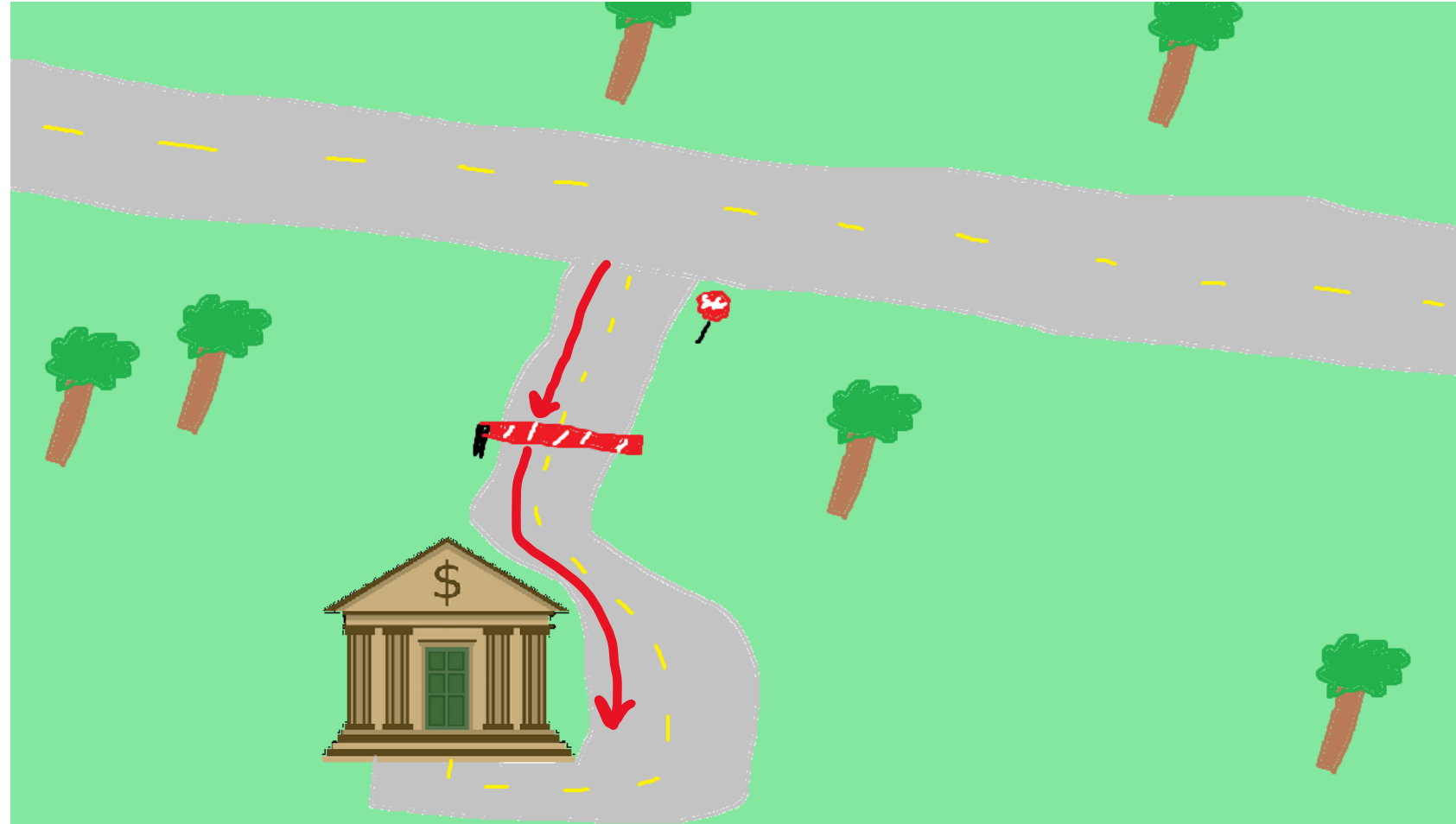
# Threat Modeling

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



# Assessing Risk

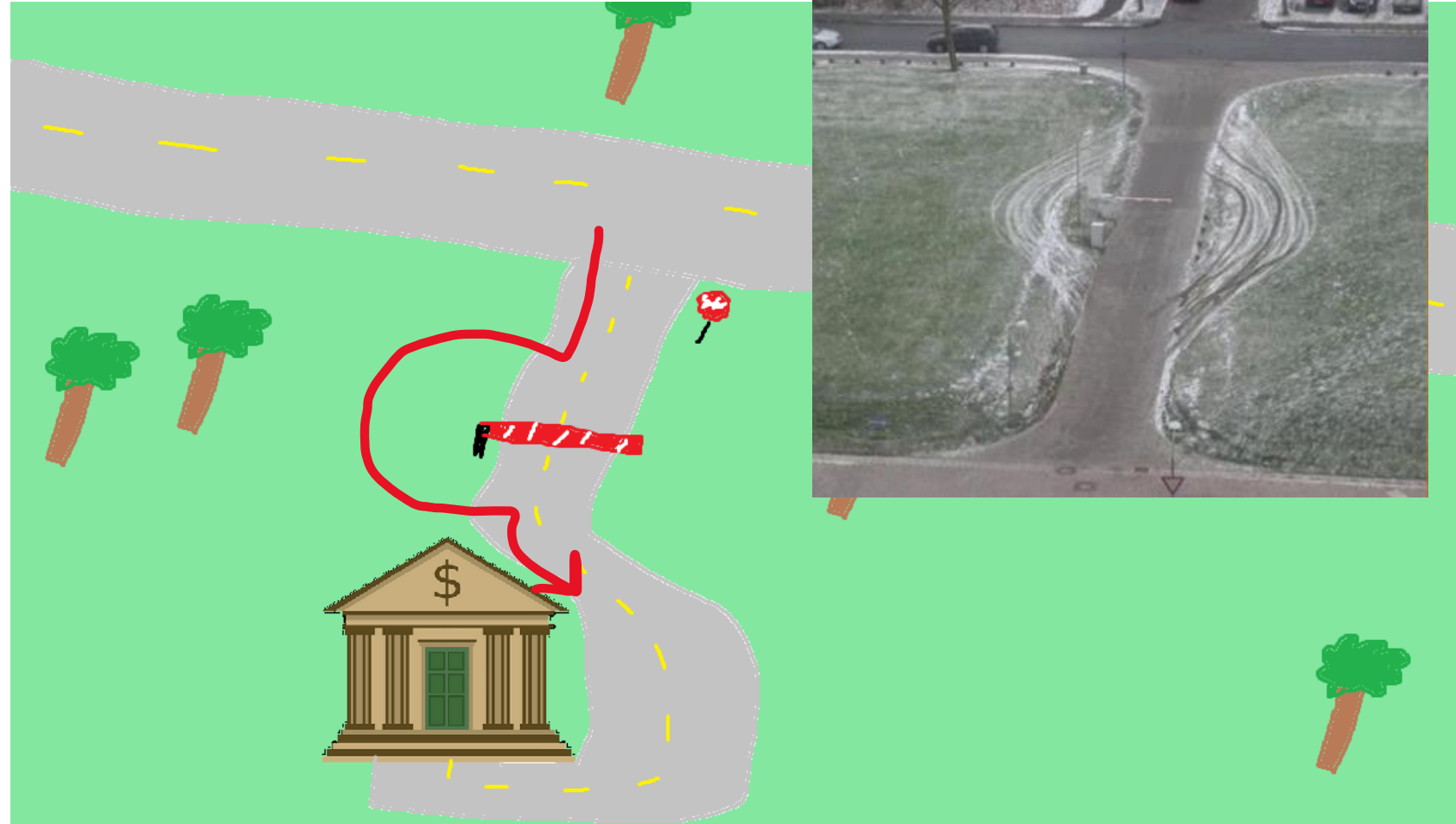
We expect users to interact with our system in a certain way



# 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

User-Id :

Password :

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 :

Password :

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 :

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 :

Password :

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 :

Password :

**LOGIN SUCCESS**



# Who do we trust?

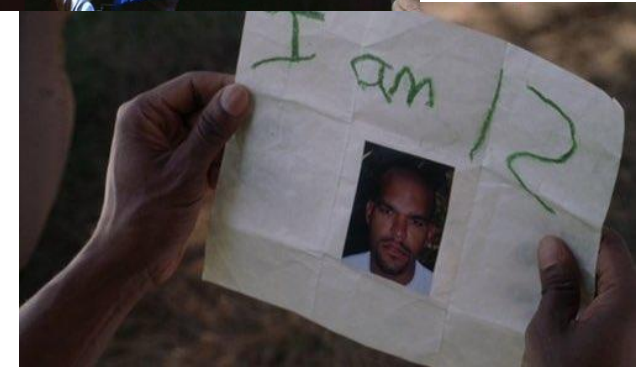


Are they honest? Are they reliable? Are they dependable? What are their intentions?



# Who do we trust?

Trust as little as possible



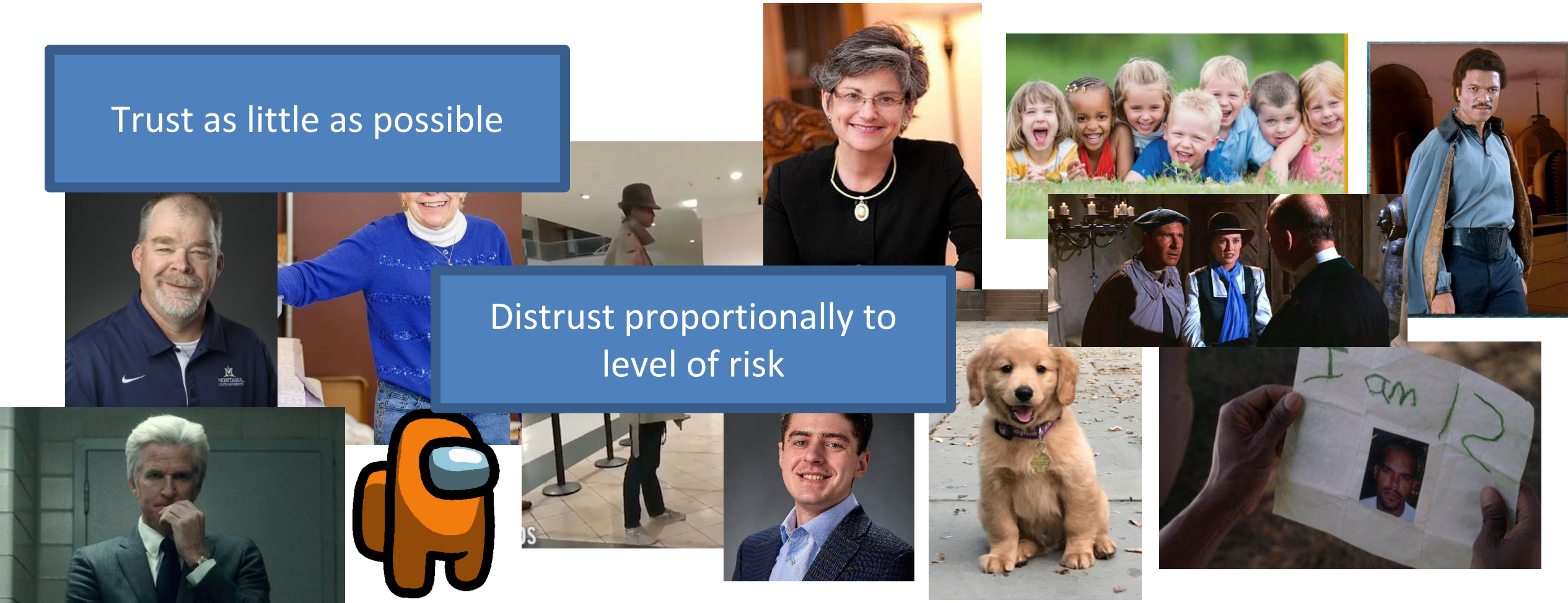
Are they honest? Are they reliable? Are they dependable? What are their intentions?



# 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?

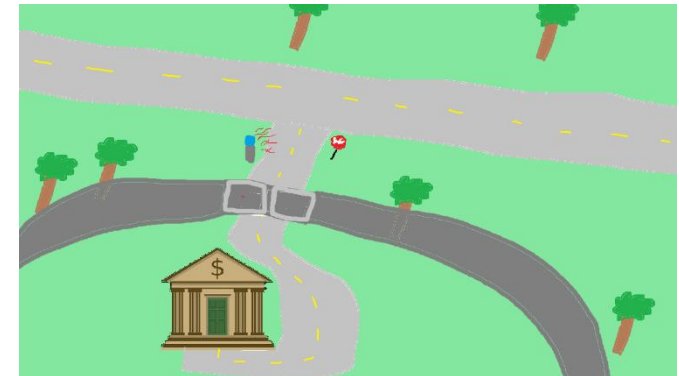
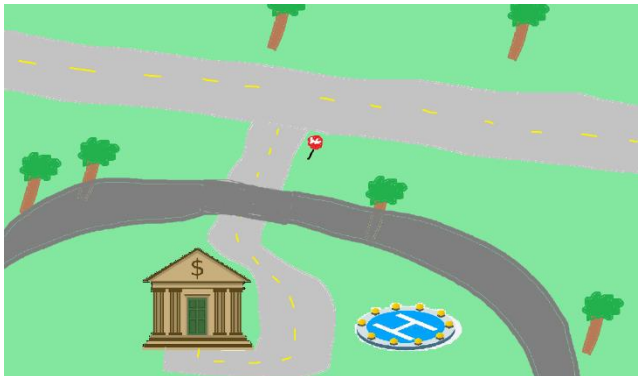
Trust as little as possible

Be aware of your technology

Distrust proportionally to  
level of risk

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

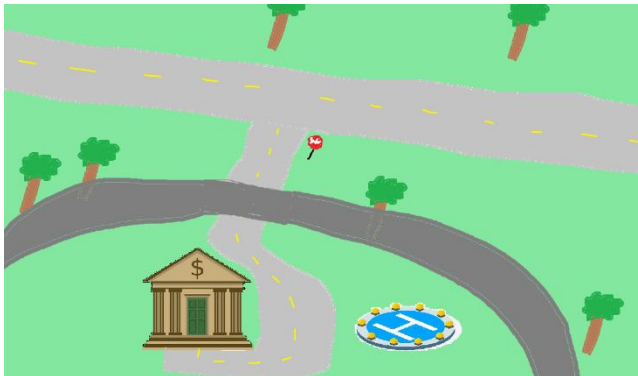
# Perfect security is impossible



# Perfect security is impossible



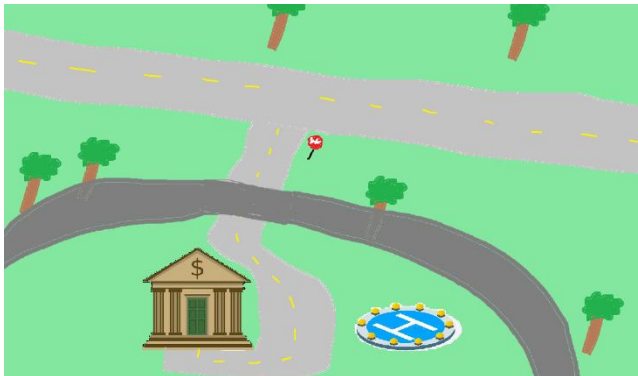
- New assets



# Perfect security is impossible



- New assets
- New threats





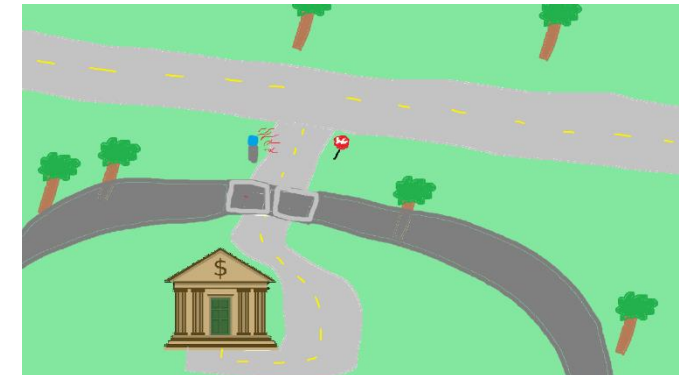
# Perfect security is impossible



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



*They fly now? They fly now*



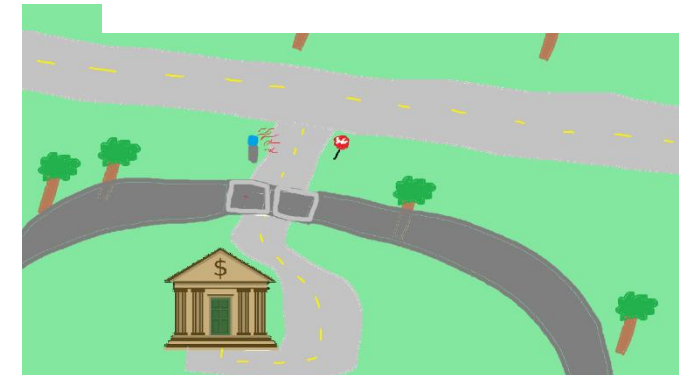
# Perfect security is impossible



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



*They fly now? They fly now*



# Perfect security is impossible

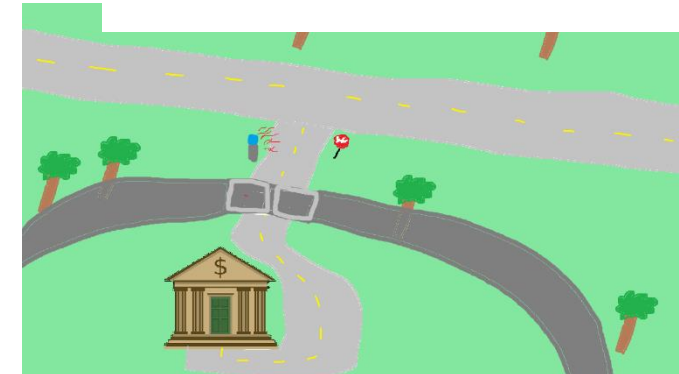


- New **assets**
- New **threats**
- New **capabilities**
- New **technology**



*They fly now? They fly now*

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



# Threat Modeling

You develop a threat model by focusing on four key questions

1. What are you building?
2. What are the assets?
3. What can go wrong?
4. What should you do about those things that can go 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 ...

What are your assets?

What can go wrong?

What things can be done to prevent those things?

If something bad happens, what can we do?

# Structured Approaches

WE NEED STRUCTURE

- 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

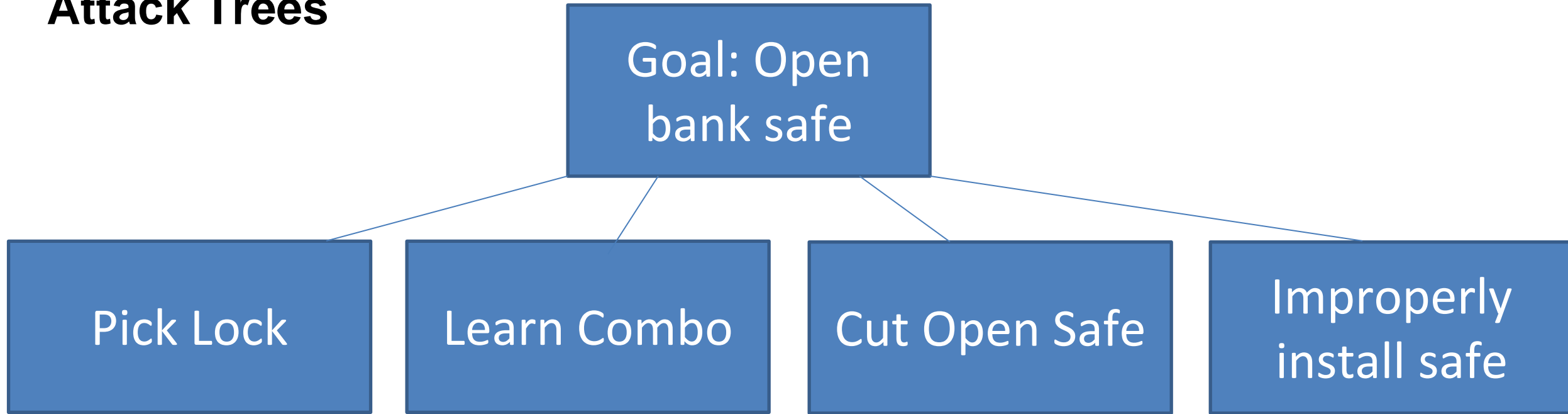
- STRIDE
  - **S**poofing, **T**ampering, **R**epudiation, **I**nfо Disclosure, **D**enial of Service, **E**levation of Privilege  
<https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats>
- Attack Trees
- Attack Lists & Libraries (ie. Common and Current vulnerabilities)

There is no “right” choice

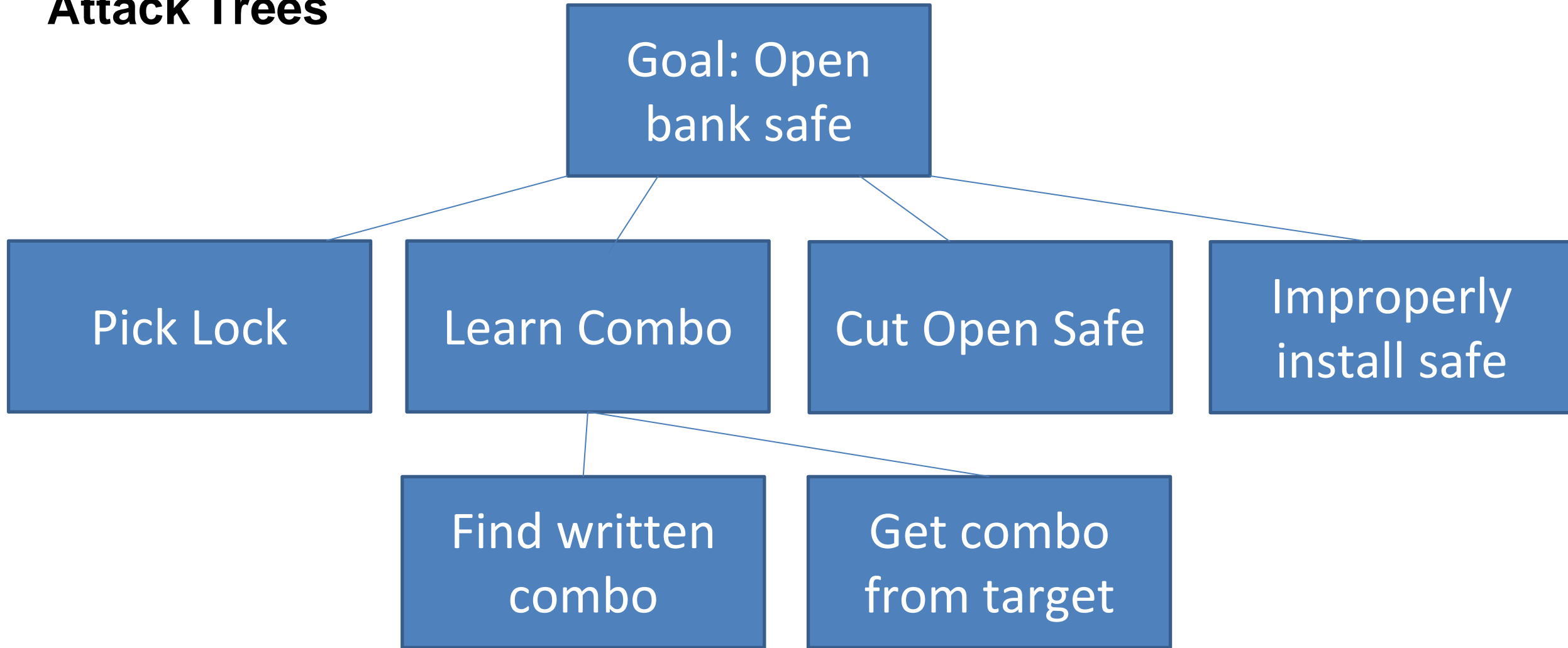
# Attack Trees

Goal: Open  
bank safe

# Attack Trees

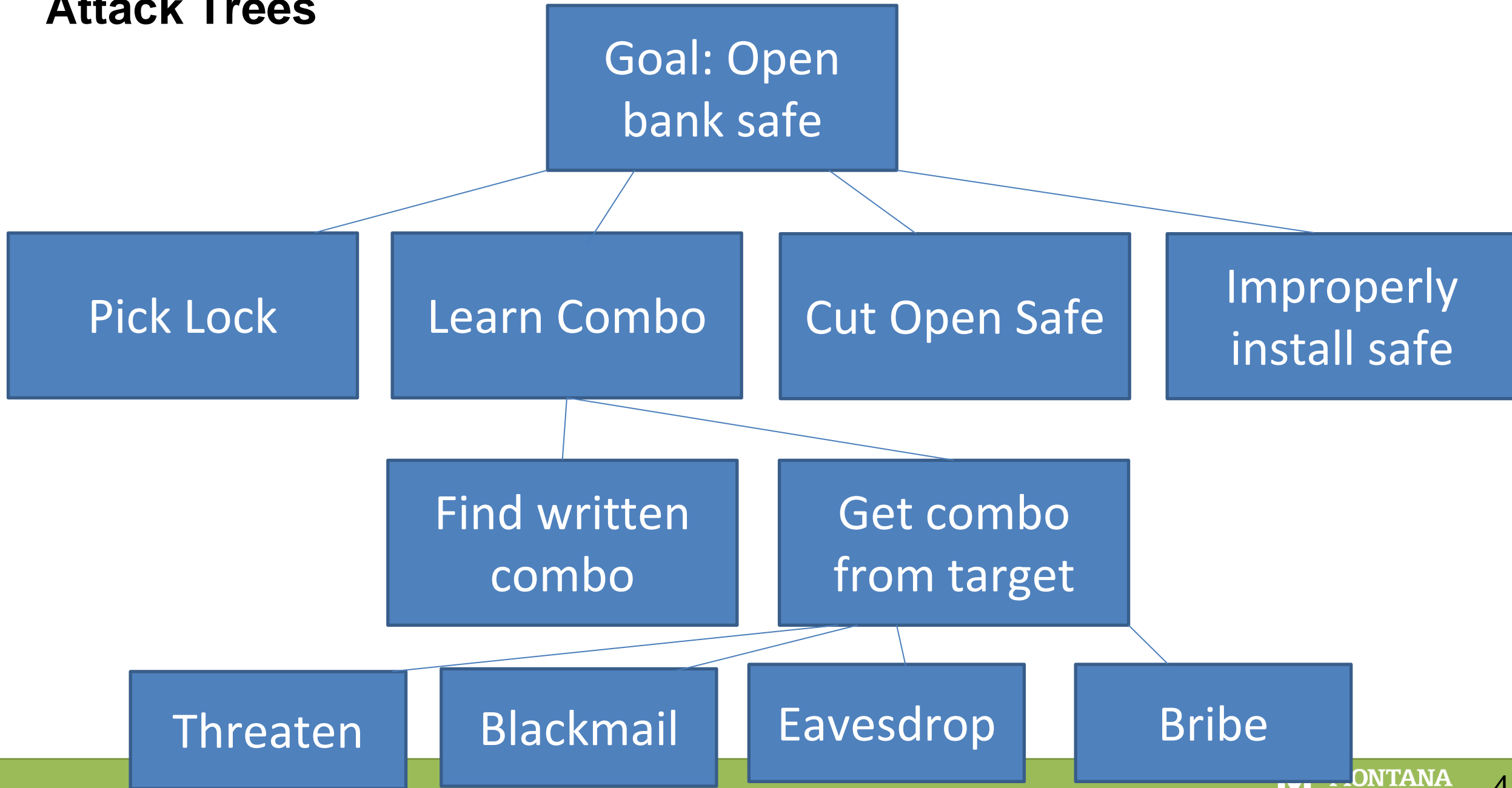


# Attack Trees





# Attack Trees



## What is Security?

Cryptography

User controls → access control permission → Weakness that can be exploited

Penetration Testing/vulnerability Assessment

IoC - Indicators of Compromise

↳ Logging

Obscurity → Defensive  
Offensive

Physical → Door locks, Guards, Access Card

## What is Not Security?

Code optimization & performance

Why is it important?

To learn about "best" coding practices

Maintain sensitive information, confidentiality

Private Code

Useability & functionality

Servers safety & Data Safety

\$

Economic & Industrial Control Systems



What are some examples of security? Something you have experienced?

Digital Forensics

Political and Global events

Password leaks

Malware → Trojans, viruses

Data leaks → Source code, Credit Cards, Healthcare

Captcha → Authentication, O-AUTH

What can we do about security issues?

Authentication, MFA

Password Managers

Good Cyber Hygiene

Antivirus Software

App + System updates



We are at a bar. We hand our phone to a cute person?

What are the assets?

Venmo Balance  
Physical phone  
Medical Health  
Passwords + Credit phone  
Contact Information  
Photos → Blackmail  
Nudes  
Authentication Device  
Social Media  
App accounts  
Reddit Account  
Amazon Account Email  
Security  
Tesla

What can go wrong?

Dropping of Phone  
Download malicious software  
Factory Reset  
Send money to themselves  
Use your social  
Order Amazon product,  
Steal Passwords, information  
Change Permissions  
Germs + Covid!  
Put illegal stuff

What can we do?

Authentication

Ask them, not give

Never share passcode

hold their phone  
or wallet as collateral

Don't leave the house

Secondary Phone

Don't keep personal  
stuff phone

monitor ask for their  
Settings phone

