

COMP435: *SECURITY CONCEPTS!*

Lecture 1: Introduction

Please don't sit in the
back 4 rows 😊

Welcome! 😊

- Target audience: COMP majors
- Pre-reqs: 210, 211, 311
- No background in security expected!

Course Goals

- Apply a security mindset
 - Evaluating the world around you, challenging assumptions
- Explain the building blocks of security
 - Basics of cryptographic primitives (integrity, confidentiality, availability)
- Evaluate a given security policy
 - Understand what policies make sense for different application domains
- Analyze security breaches in the news
 - Learn from history + past mistakes
- Ask the “newbie” questions
 - Knowing *what to ask* when you are unfamiliar with a new platform or technology

Why study security?

- Practical knowledge for all of your professional careers.
- Don't want security experts to just be a few powerful people!
- Economic and real-world stakes.
- Security is socio-technical, not purely technical.
- Also, this course will provide supplemental background for other computer science areas

My goals/hopes!

- You all will be inspired to take other awesome electives in our department after each related unit:
 - *Crypto: COMP 437*
 - *Software Engineering: 423/523*
 - *OS: COMP 530*
 - *Compilers: COMP 520*
 - *Networking: COMP 431*
- Leave the course with:
 - A baseline of security literacy.
 - Confidence in analyzing and reasoning about security risks.
 - Practical knowledge for your careers!

Syllabus!

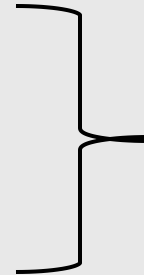
Course site:

<https://www.cs.unc.edu/~kakiryan/teaching/435-fa25/435-fa25.html>

Course Structure

■ Assessment (50%):

- *6x Quizzes: 40%*
- *Final Exam: 10%*



Your final can replace up to two of your lowest quiz scores.

■ Practice (35%):

- *6x Written Assignments: 15%*
- *5x Labs: 20%*

■ Final Project (15%):

- *Proposal: 5%*
- *Final Presentation: 10%*

Course Outline: ~6 Units

- Introduction to Security Concepts + Principles
- Cryptography
- Systems/OS Security
- Software Security
- Network Security
- Web Security
- *Bonus* Misc Unit at the End 😊

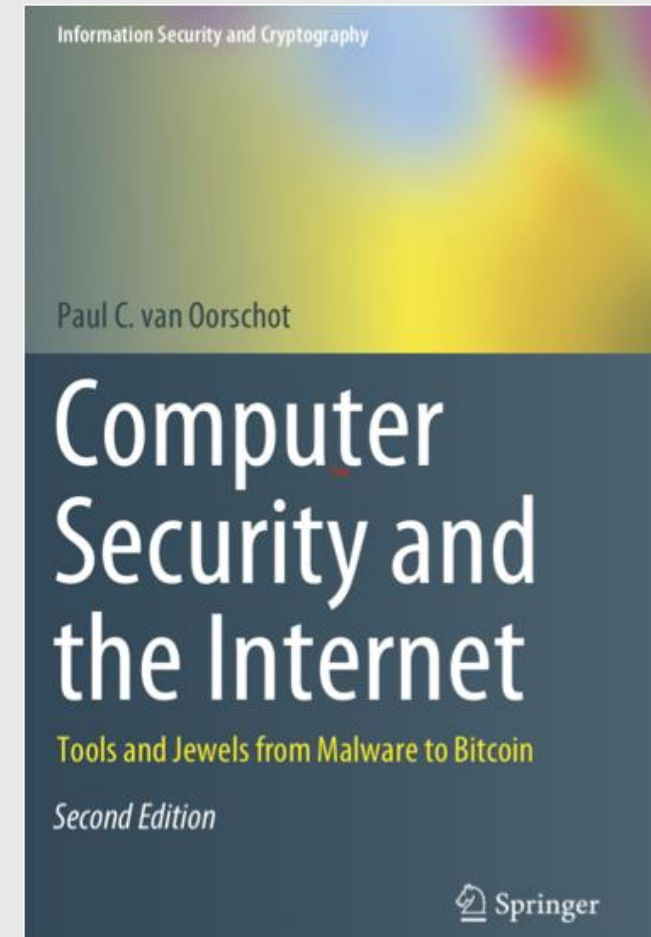
Course Outline: ~6 Units

■ Each unit:

- Gives a taste of a security sub-area. There will always be more to explore! 😊
- 1 written assignment. Practice problems to reinforce concepts. This will provide practice for the quiz. Students will submit handwritten solutions to Gradescope.
- 1 lab. Involve deeper exploration of the security subarea through guided tutorials and programming exercises. Students will submit typed lab reports and code to Gradescope.
- 1 quiz. 30 minutes of at the start of class. Similar problems are seen in the written assignment and pre-released practice problems.

Textbook

- “Computer Security and the Internet,” Paul C. van Oorschot
- Readings posted before class
- PDF available online





ADMINISTRATIVE DETAILS

Extensions + Late Days

- You have 8 days to use on any assignment in the course, with no explanation needed.
- You may request extensions for illness or personal life events so you don't have to use up your late days.
 - Extension form is linked in the syllabus
- If you are not sure if something qualifies for an extension, just fill out the form anyway, and we will get back to you.
- *You will not be penalized for submitting the assignment within the provided grace period if you receive an extension!*

Gradescope

- Make sure you are enrolled!

The Team!

- TA: Jacob Brown
- LAs: William Millen & Christopher McClanahan
- TA/LA office hours will be held in CSXL RM SN137. Time TBD!
 - I will send out an announcement once we schedule them!
- My office hours are 10-12 in FB114.



HEALTH & SAFETY

Face Masks

- Optional
- Use a mask often!

Emergency Procedures

- Evacuate (fire, chemical hazard)
- Shelter in place (weather related)
- Secure in place (armed and dangerous assailant)
 - run, hide (secure in place), fight

Act Ethically

You may not attempt to break into any system that is not your own; you may not attempt to thwart or circumvent the security of any system that is not your own.

Doing so is, at a minimum, a violation of the honor code and likely a violation of the law.

Acknowledgements

- “Computer Security and the Internet,” Paul C. van Oorschot
- “Security in Computing,” Pfleeger, Pfleeger, Margulies
- “Introduction to Modern Cryptography,” Katz, Lindell
- Cynthia Sturton 😊



BASIC PRINCIPLES



“A SECURITY MINDSET MEANS
LOOKING BOTH WAYS BEFORE
CROSSING A ONE-WAY STREET”

-- Unknown, Doug Linder, Laurence J. Peter
(an apparent chain of misquotes).

Q: What are your **assumptions**
about a one-way street?

The Security Mindset

- Definition: noticing and challenging (often unstated) assumptions.
- Goal of this course: ***To Develop a Security Mindset!***
- Factors to consider:
 - *Security policies*
 - *Adversarial actions*
 - *Risk*
 - *Role of design and usability*
 - *End-user's responsibility*

SO.... WHAT DO WE MEAN BY SECURITY??

In this class, we will be learning
about *secure computer systems*.

A Secure System:

- Prevents harm.
 - *Harm is context-dependent.*
- Protects its resources in accordance with a given policy
 - *Even in the presence of an ***adversary!****

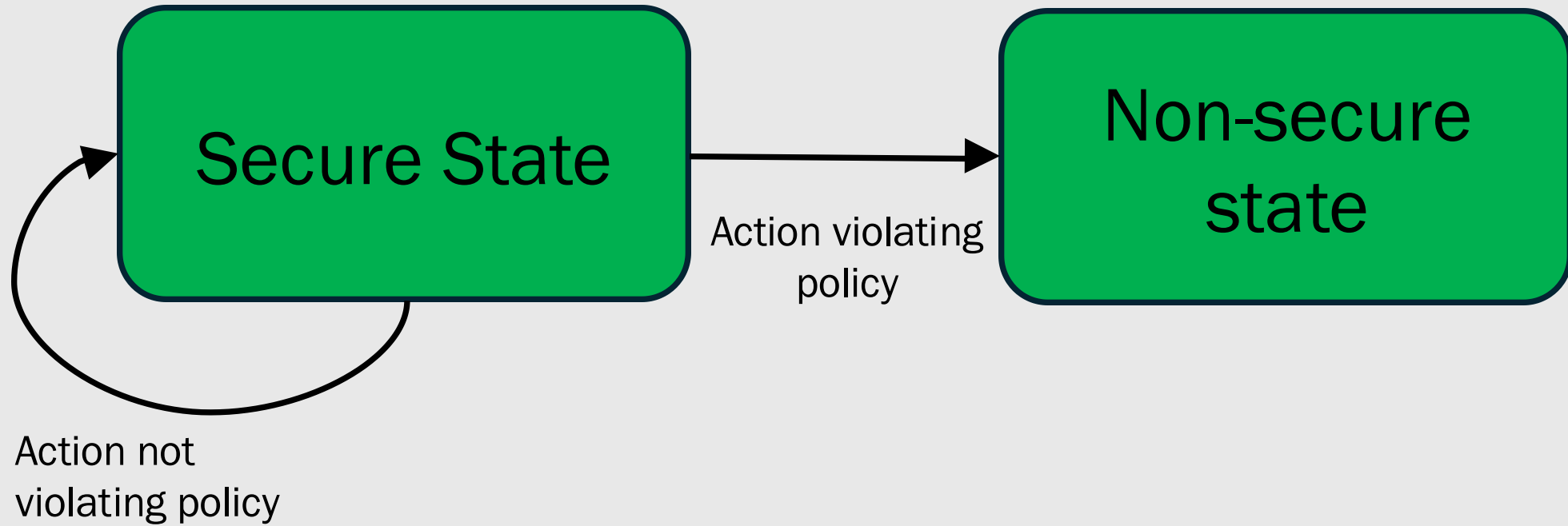
A Secure System:

- Prevents harm.
 - *Harm is context-dependent.*
- Protects its resources in accordance with a given policy
 - *Even in the presence of an ***adversary!****

Security Policy

- Specification of what should and should not be allowed.
- Assessing security is done with respect to a policy.
 - Required for designing and evaluating secure systems.
- Different from the mechanism (implementation).
 - This course: mostly mechanism – the easy part!

Theory vs. Practice



A Secure System:

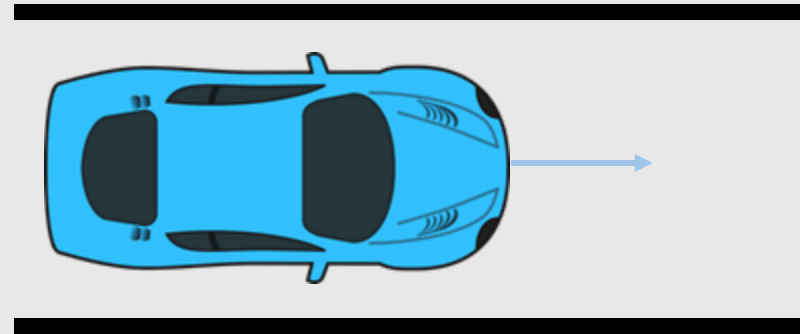
- Prevents harm.
 - *Harm is context-dependent.*
- Protects its resources in accordance with a given policy
 - *Even in the presence of an ***adversary!****

Adversaries

- Definition: the source or threat agent behind a potential attack
 - Often called an **attacker** (once threat activated into actual attack)
- Accidental vs. malicious
 - Both dangerous
 - Different outcomes and prevention strategies

Accidental

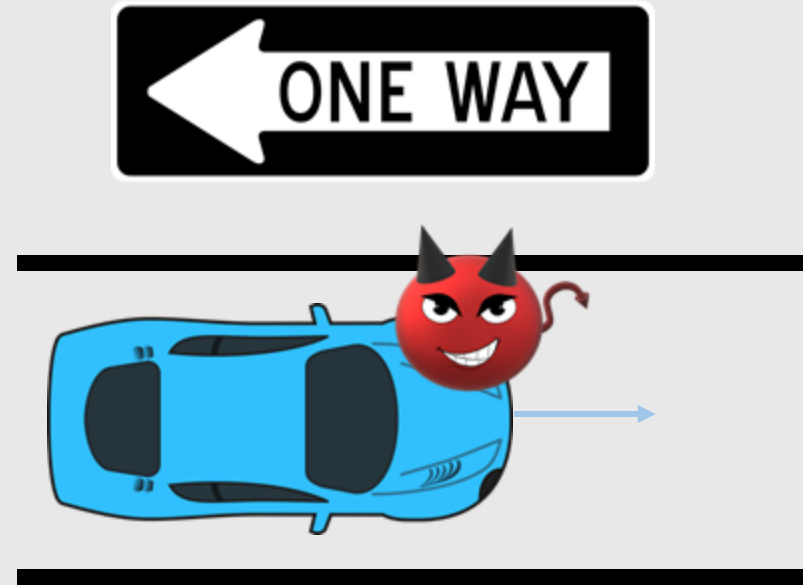
- Prevention:
 - Road signs
 - Road design
- Consequences:
 - Traffic build-up



Malicious

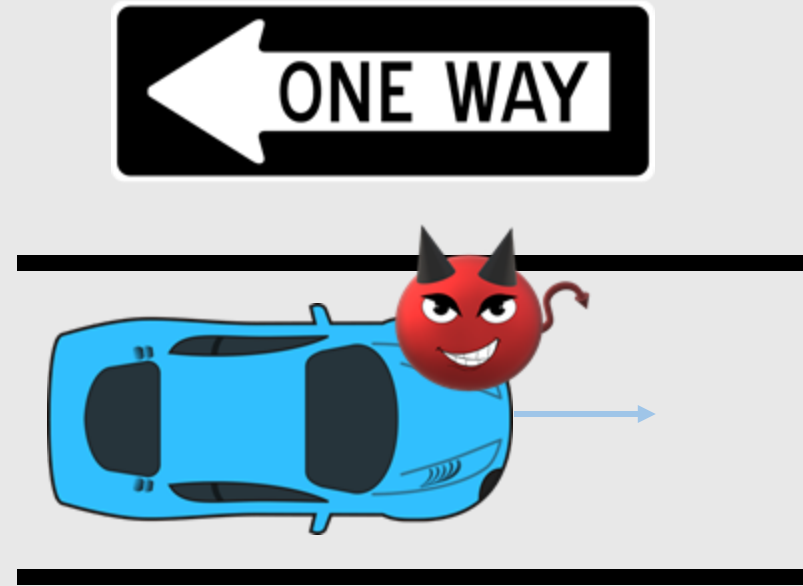
Prevention:

- ~~Road signs~~
- ~~Road design~~



Malicious

- Prevention:
 - *Barricades*
 - *Gated entry & exit points*
- Consequences
 - Fatalities



A Secure System:

- Prevents harm.
 - *Harm is context-dependent.*
- Protects its resources in accordance with a given policy
 - *Even in the presence of an *adversary!**

Q: What is a resource in the computer security context?

Resources

- Definition: Assets we wish to protect

laptops, phones,
smart cards, storage
disks, CPUs, physical
cables, routers,
bridges

Hardware

operating systems,
apps, utilities,
database
management
systems, js running in
a browser

Software

files, databases,
passwords,
cryptographic key
material

Data

3 Policy Primitives for Evaluating Secure Systems

- Prevents harm.
 - *Harm is context-dependent.*
- Protects its **resources** in accordance with a given **policy**
 - *Even in the presence of an ***adversary!****

3 Policy Primitives for Evaluating Secure Systems

- Confidentiality

- Integrity

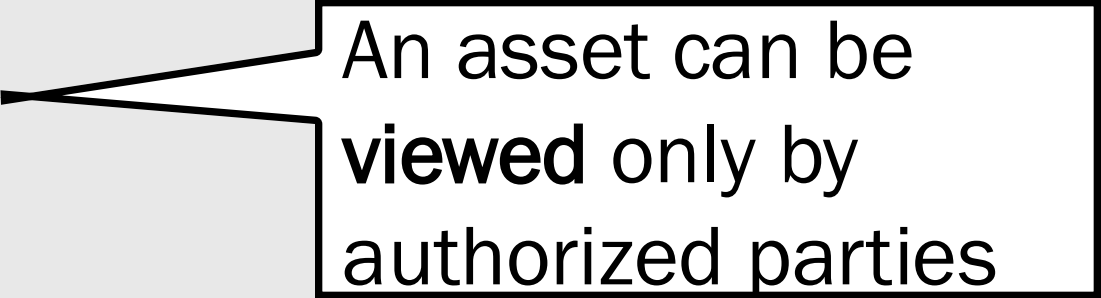
- Availability



C.I.A. triad

3 Policy Primitives for Evaluating Secure Systems

- *Confidentiality*



An asset can be
viewed only by
authorized parties

- Integrity


- Availability

3 Policy Primitives for Evaluating Secure Systems

- Confidentiality

- *Integrity*

- Availability



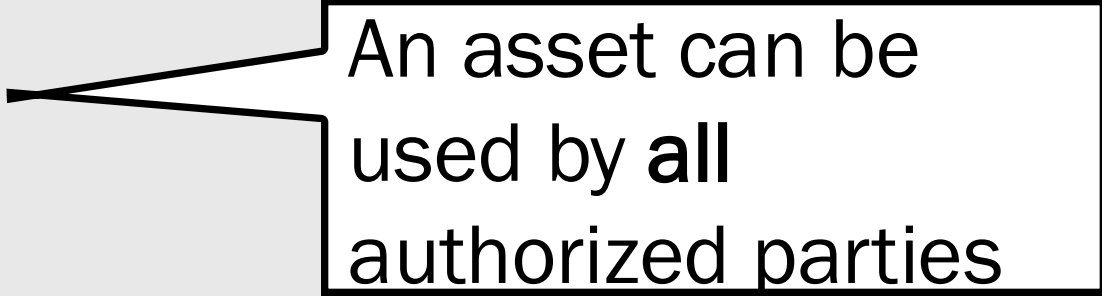
An asset can be
modified only by
authorized parties

3 Policy Primitives for Evaluating Secure Systems

- Confidentiality

- Integrity

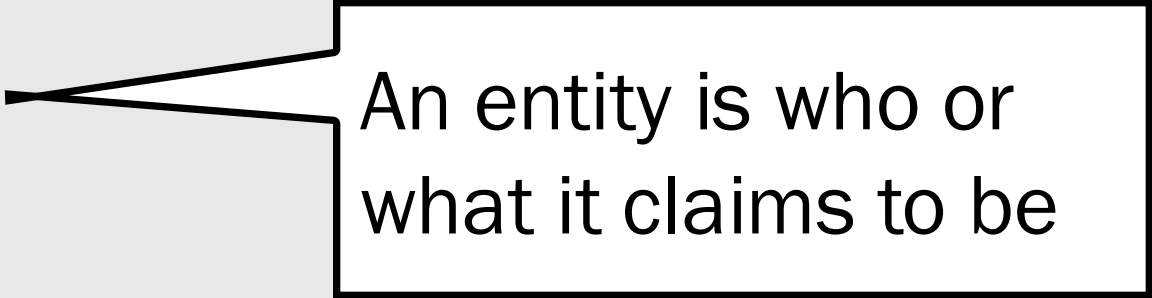
- *Availability*



An asset can be
used by **all**
authorized parties

2 more primitives

- *Authentication*



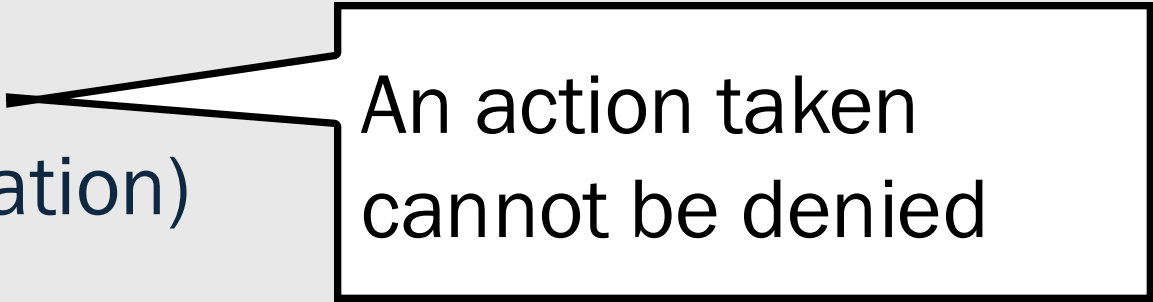
An entity is who or
what it claims to be

- Accountability
(a.k.a. non-repudiation)

2 more primitives

- Authentication

- ***Accountability***
(a.k.a. non-repudiation)



An action taken
cannot be denied

Practice Problems!

- Take 7 minutes to complete the problems with 1-2 classmates.
- As a reminder, the security primitives are:
 - *Confidentiality*
 - *Integrity*
 - *Availability*
 - *Authentication*
 - *Accountability*



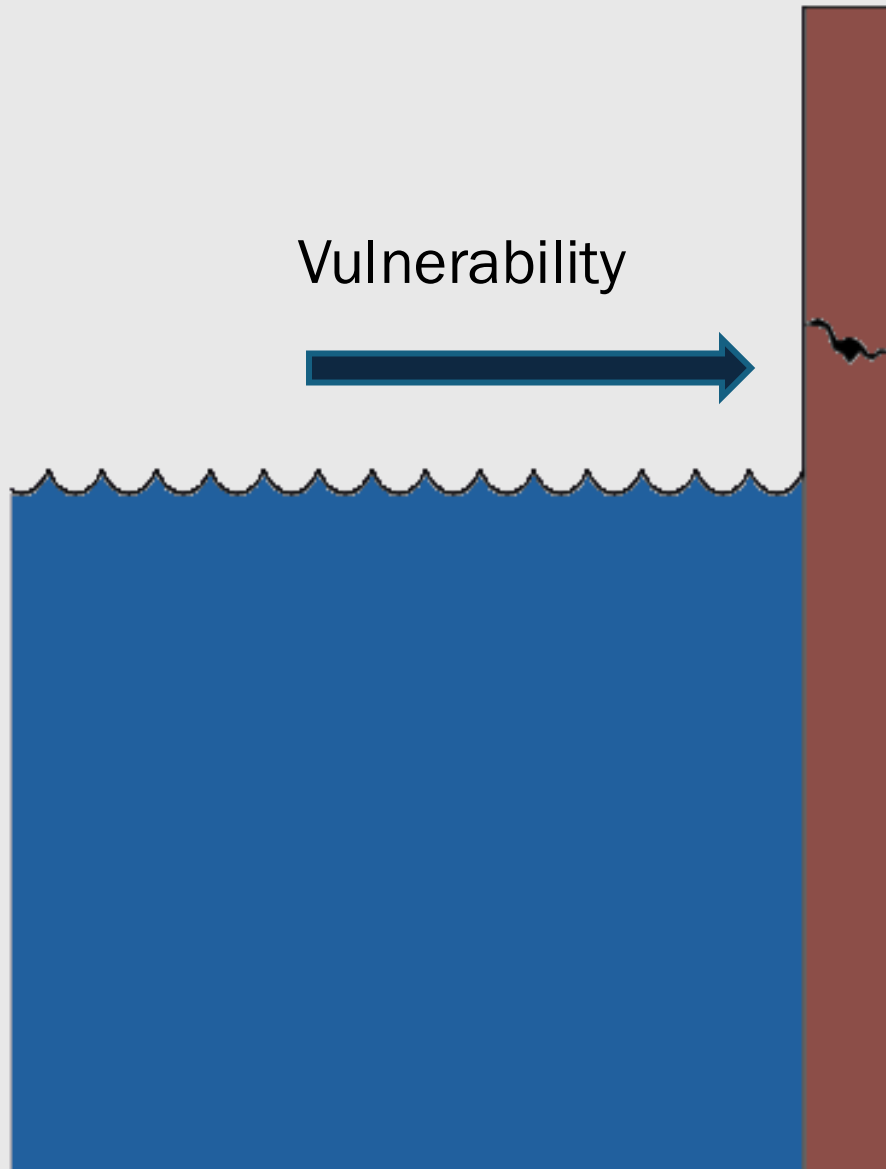
THREATS, ATTACKS, AND COUNTERMEASURES



Threat



Vulnerability



Potential Harm:

- getting wet
- drowning



Some terminology

- Harm: a violation of a desired security policy
 - Ex: getting wet or drowning
- Vulnerability: a weakness that could be exploited to cause harm
 - Ex: a crack in the wall
- Threat: a set of circumstances that could cause harm
 - Ex: Water that might overflow or cause the wall to collapse

Policy:

- only family members and their guests may enter
- only family members can take objects out of the house



Threats

Vulnerabilities

Harm

Policy:

- only family members and their guests may enter
- only family members can take objects out of the house



Threats

Curious
passers-by

Vulnerabilities

Door is open

Harm

Stranger
walks in off
the street

Turn to your neighbor and answer
Q2 on the worksheet