# Section 1:

# Threat Modeling

# TA Introduction

Wenqing Lan (lanw3@cs.washington.edu) Bowen Xu (bwx074@cs.washington.edu)
Hanfei Chen (hanfec@cs.washington.edu) Karman Singh (shubhs2@cs.washington.edu)
Tony Wang (zihongw@cs.washington.edu) Philip Garrison (philipmg@cs.washington.edu)
Matt Ziegler (mattzig@cs.washington.edu) Edan Sneh (esneh@cs.washington.edu)
Preferred email: cse484-tas@cs.washington.edu

Office Hours

- **Mondays 11:30am - 12:00pm:** David Kohlbrenner - CSE2 310
- **Tuesdays, 10:30-11:30am:** Edan, Matt, Philip - room TBD
- **Wednesdays, 5pm-6pm:** David C., Matt, Zihong - Zoom
- **Thursdays, 5pm-6pm:** Wenqing, Karman, Bowen - room TBD
- **Fridays, 2:30pm-3:30pm:** David C., Philip, Wenqing room TBD + Zoom

# Administrivia

What's assigned?

- In-class activities (canvas "quizzes" during breakouts)
- 3 Homeworks (HW1 due October 8)
- 3 Labs
- Weekly Research Paper Readings for M 584 students (or EC for 484)
- Final project

# Student Resource List

(See course website, under Administrivia)

## Additional Resources

**Disability Accommodations**

Embedded in the core values of the University of Washington is a commitment to ensuring access to a quality higher education experience for a diverse student population. Disability Resources for Students (DRS) recognizes disability as an aspect of diversity that is integral to society and to our campus community. DRS serves as a partner in fostering an inclusive and equitable environment for all University of Washington students. The DRS office is in 011 Mary Gates Hall.

Please see the UW resources at http://depts.washington.edu/uwdrs/current-students/accommodations/.

**Religious Accommodations**

Washington state law requires that UW develop a policy for accommodation of student absences or significant hardship due to reasons of faith or conscience, or for organized religious activities. The UW's policy, including more information about how to request an accommodation, is available at Religious Accommodations Policy. Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form https://registrar.washington.edu/students/religious-accommodations-request/.

**Sexual Harassment**

University policy prohibits all forms of sexual harassment. If you feel you have been a victim of sexual harassment or if you feel you have been discriminated against, you may speak with your instructor, teaching assistant, the chair of the department, or you can file a complaint with the UW Ombudsman's Office for Sexual Harassment. Their office is located at 339 HUB, (206)543-6028. There is a second office, the University Complaint Investigation and Resolution Office, who also investigate complaints. The UCIRO is located at 22 Gerberding Hall.

Please see additional resources at http://www.washington.edu/about/ombudsman/role.html and http://f2.washington.edu/treasury/riskmgmt/UCIRO.

**WISE: Women In Science and Engineering**

Women in Science and Engineering (WiSE) is a university-level program housed within the Center for Workforce Development, designed to increase the recruitment and retention of women of all ethnic backgrounds in science and engineering (S&E) and to create an academic and social climate at the UW which is conducive to both men and women in S&E at the undergraduate and graduate levels.

Please see additional information at http://www.engr.washington.edu/curr_students/studentprogs/wise.html.

# Icebreaker

In groups of 3 or 4, share your answers to the following questions:

- What is your name?
- Why are you taking this class?
- Have you had any experiences with computer security and privacy in your personal life?

# What is threat modeling?

- An approach for analyzing the security of a computer system
- Examine the potential vulnerabilities and risks of the system, and how attackers might approach it
    - *What are we protecting?*
    - *What does an attacker have to gain?*
    - *How would an attacker try to exploit the system?*

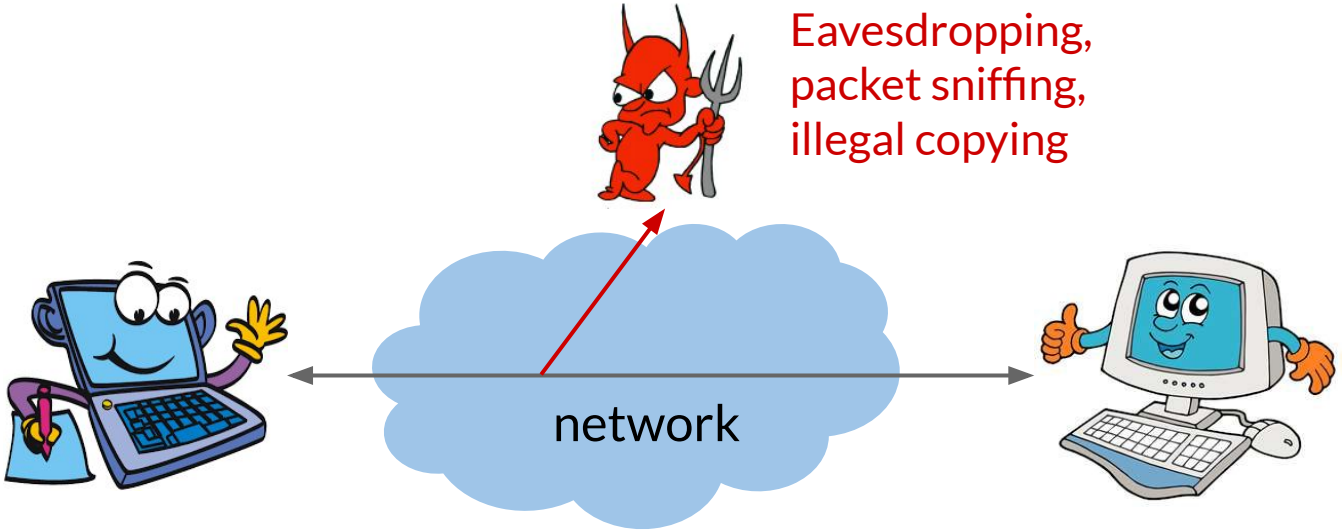
# What does it mean to be “secure”?

The traditional goals of security are:

- Confidentiality
- Integrity
- Authenticity
- Availability

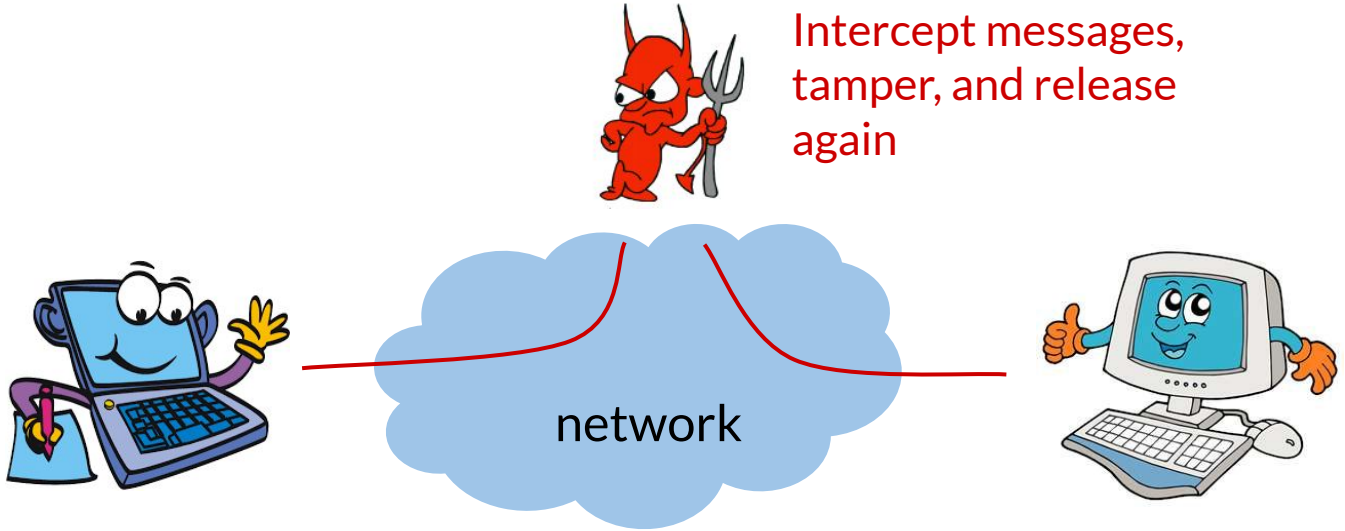
# Confidentiality

Confidentiality is the *concealment of information*



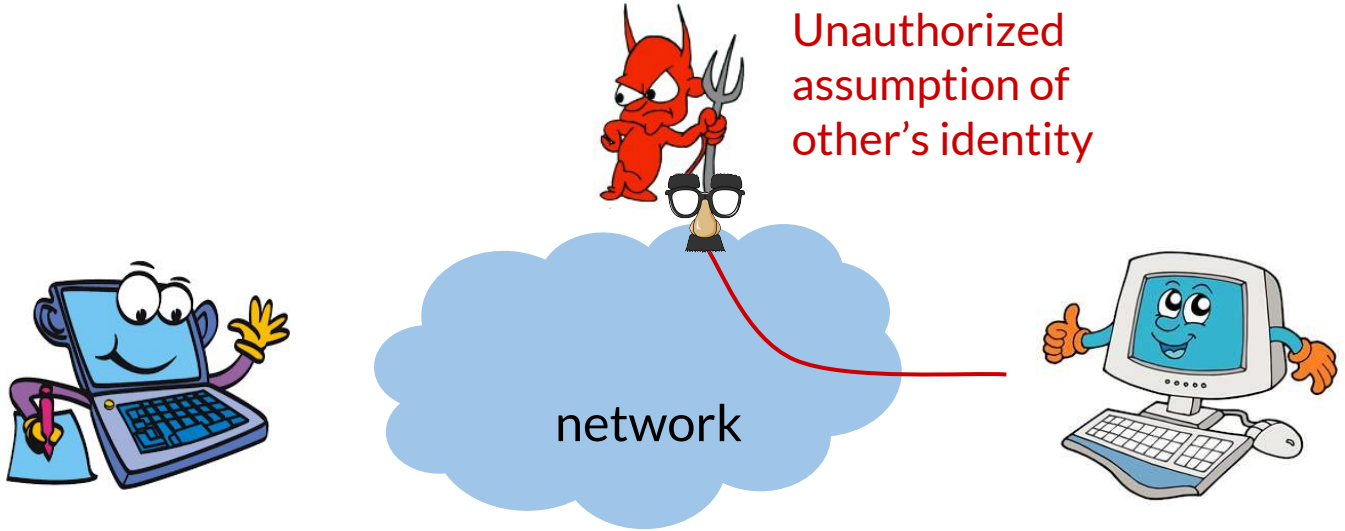
# Integrity

Integrity is the *prevention of unauthorized changes*



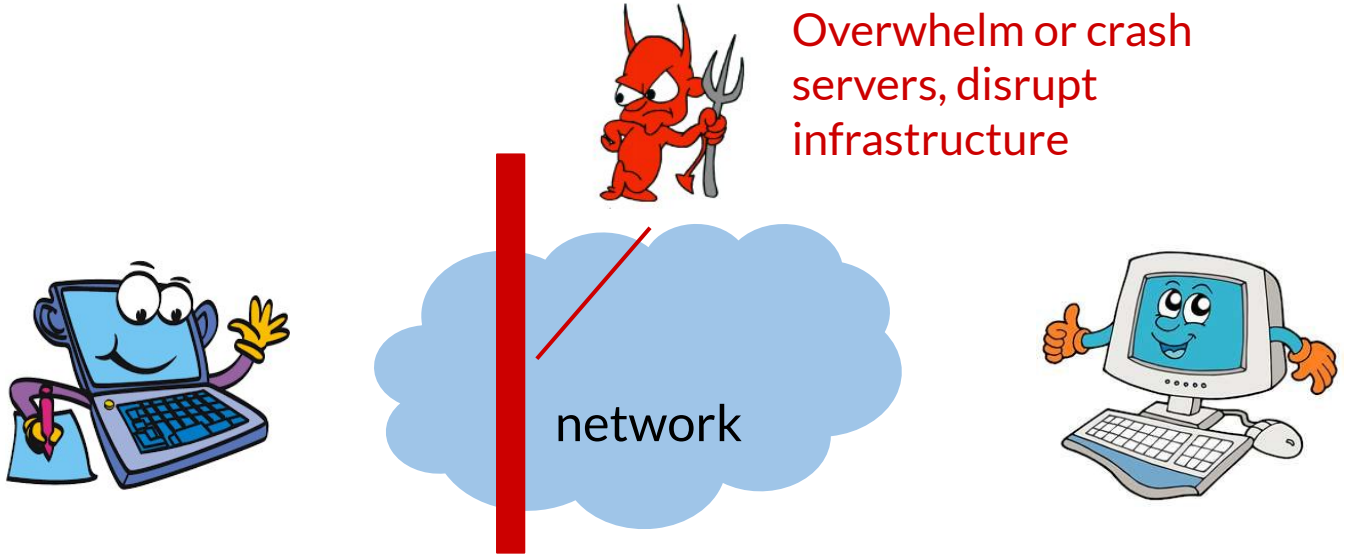
# Authenticity

Authenticity is *knowing who you're talking to*



# Availability

Availability is the *ability to use information or resources*



# Threat Modeling Example: Social Media Services

**Tip**

Be aware what information you are giving away

Be aware how they are being used

# Threat Model

- **Assets**
  What are we trying to protect? How valuable are those assets?
- **Adversaries**
  Who might try to attack, and why?
- **Vulnerabilities**
  How might the system be weak?
- **Threats**
  What actions might an adversary take to exploit vulnerabilities?
- **Risk**
  How important are assets? How likely is an exploit?
- **Possible Defenses**

# Assets

What are we trying to protect?

- User Data
  - Personal Info (Date of birth, SSN, phone #)
  - User generated content (messages, photos, posts)
  - Ad targeting information

How valuable are those assets?

- Potentially very personal
- Cannot be measured by money

# Adversaries

## Who might try to attack, and why?

- Foreign governments
- Other companies
- Hackers
- Employees
- Other users

**Tip**

Some adversaries might not be obvious. Users misuse can also cause unintentional problems.

# Vulnerabilities & Threats

How might the system be weak?

How might an adversary exploit vulnerabilities?

- Code vulnerabilities
- Weak passwords
- Social engineering
- Insider threats (employees)
- Physical threats

# Risks

How important are assets?

- Legal and ethical aspects
  - Legal ramifications
  - Company reputation
  - Personal information of customers

How likely is a successful attack?

- How many resources would the adversary need to execute an attack?
- Can deter, but attackers have asymmetric advantage

# Asymmetric Advantage

An attacker only needs to win in one place.

# Defense-in-depth

- Write code using secure tools and practices
- Store only the information you need to store
- Limit employee access to user data
- Enforce strong password rules for users

# Section Activity:

Adversarial thinking about design assumptions

https://docs.google.com/document/d/1rYJQPjAIJ_EGFgWULXTtmM9AFdS7CTMU0AtGVXSMisQ

# Some examples of systems....

## Echo Dot


## Grocery store self checkout

## Self-driving cars

# Section Student Survey

https://canvas.uw.edu/courses/1477394/quizzes/1532288

Please fill out this quick survey on Canvas to help us help you learn!

- Name
- Preferred Pronouns
- What helps you participate in class?
- Is there anything we should know to help you learn?

# Reminders!

- Find people to work with! [Up to 3 people per group]

- Check discussion board regularly!