

# **CSE 484 / CSE M 584: Computer Security and Privacy**

Fall 2022

Franziska (Franzi) Roesner  
franzi@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...



# Hello 😊

- Instructor: Franziska (Prof. Franziska Roesner) (she/her)
- Staff:
  - David Chen
  - Theo Gregersen
  - Aroosh Kumar
  - Wenqing Lan
  - Tim Mandzyuk
  - Noah Ponto
  - Basia Radka
  - William Travis
  - Julia Wang



Theo



Aroosh



Wenqing



Tim



Basia



William



Julia



# Course Plan

- Lectures and Sections and (most) Office Hours in-person
  - Lectures are recorded (please attend!)\*
    - \* Sections may be only partially recorded
    - \* Office hours will not be recorded
    - \* Recordings include student questions and should not be shared outside the class
  - Access the recordings via Canvas
- Largely the same curriculum as usual
  - Labs and homeworks and final project; **no exams**
  - We will adapt throughout the quarter as needed
- If you are struggling with anything, let us know!

# Course Resource Cheat Sheet

- **In Person:** Lectures, sections, office hours (planned)
- **Zoom:** Limited office hours (planned)
- **Canvas:** Links to recordings, assignment submissions, grades
- **Course website:** Schedule, assignment details, readings, policies
- **Ed:** Discussion board
- **Course mailing list:** Announcements (though most go to Ed)
- **Email:** Reach course staff privately (generally best: `cse484-tas@cs`)

# What Does “Security” Mean to You?

Try putting some answers in <https://pollev.com/franziroesner>

# What are topics you are excited about?

- It is also okay if you don't know what topics you are interested in yet!
- The course's final project will give you the opportunity to explore something not covered in class in depth.

Try putting some answers in <https://pollev.com/franziroesner>



# How Systems Fail

Systems may fail for many reasons, including:

- **Reliability** deals with accidental failures
- **Usability** deals with problems arising from operating mistakes made by users
- **Design and goal oversights** deals with oversights, errors, and omissions during the design process
- **Security** deals with **intentional** failures created by **intelligent** parties
  - Security is about computing in the presence of an adversary
  - But **security, reliability, usability, and design/goals oversights** are all related

# Challenges: What is “Security”?

- What does **security** mean?
  - Often the hardest part of building a secure system is figuring out what security means (“threat modeling”)
  - Who are the **stakeholders** for which we are considering “security”?
  - What are the **assets** to protect?
  - What are the **threats** to those assets?
  - Who are the **adversaries**, and what are their **resources**?
  - What is the **security policy or goals**?
- **Perfect security does not exist!**
  - Security is not a binary property
  - Security is about risk management

Multiple assignments and activities are designed to exercise your thinking about these issues.

# Privacy?

- Privacy often strongly overlaps security
- Privacy may also consider when systems *work as intended!*
- Not a hard-and-fast distinction
  - Privacy and security are generally intertwined
  - They might sometimes (but not always) be at odds

# Two Key Themes of this Course

1. How to **think** about security and privacy
  - The “Security Mindset” – a “new” way to think about systems
  - (This mindset will be valuable even outside of the security context, e.g., to consider diverse stakeholders of a system)
2. **Technical aspects of security and privacy**
  - Vulnerabilities and attack techniques
  - Defensive technologies
  - Topics including: software security, cryptography, malware, web security, web privacy, smartphone security, authentication, usable security, anonymity, physical security, security for emerging technologies



# Theme 1: Security Mindset

- Thinking critically about designs, **challenging assumptions**
- Being **curious**, thinking **like an attacker**, exploring **use cases not considered by the designers**,
- “That new product X sounds awesome, I can’t wait to use it!” versus “That new product X sounds cool, but I wonder what would happen if someone did Y with it; I wonder if the designers thought of Z...”
- Why it’s important
  - **Technology changes**, so learning to **think like a security person** is more important than learning specifics of today’s systems
  - Will help you **design better systems/solutions**
  - Interactions with **broader context**: law, policy, ethics, etc.

# Security Mindset Example



# Security Mindset Example



# Learning the Security Mindset

- Several approaches for developing “The Security Mindset” and for exploring the broader contextual issues surrounding computer security
  - Homework #1
    - Security reviews and ethics reflections
    - May work in groups of up to 3 people (groups are encouraged – **lots of value in discussing security with others!**)
  - In class/section discussions and activities
  - Participation in Ed discussion board (e.g., thoughts and questions about news stories, technologies)



# A Word on Groupwork

- *Strongly* encouraged, in some cases required
  - Beneficial to practice working in groups
    - Especially if you don't like it 😊
  - Attack-based labs require some creativity, where group interactions can help generate ideas
- (Please follow all the usual in-person contact guidelines 😊)

# What This Course is Not About

- Not a comprehensive course on computer security
  - Computer security is a broad discipline!
  - Impossible to cover everything in one quarter
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read news, ask questions, discuss on Ed
- Not a course on ethical, legal, or economic issues
  - We will touch on these issues, but the topic is huge
- Not a course on how to “break into” systems
  - Yes, we will learn about attacks ... but the ultimate goal is to develop an understanding of attacks so that you can build more secure systems

# Security: Not Just for PCs



smartphones



voting machines



EEG headsets



medical devices



wearables



RFID



mobile sensing  
platforms



cars



game platforms



airplanes

# Communication

- [franzi@cs](mailto:franzi@cs)
  - Use this (or instructor office hours) if something is sensitive, personal, confidential, etc.
- [cse484-tas@cs.washington.edu](mailto:cse484-tas@cs.washington.edu)
  - Best method to reach all course staff (including instructor)
- Ed Discussion Board
  - Use this if other students in the class would benefit from your question/answers  
[common case]
- Course mailing list: [multi\\_cse484a\\_au22@uw.edu](mailto:multi_cse484a_au22@uw.edu)
  - We'll use this (and Ed) for announcements
- We will do our best to be responsive, but **please be professional**, and plan ahead!



# Course Materials

- Readings:
  - No textbook; I'll be posting reading materials as we go
  - Some optional, some **strongly recommended**
- Attend lectures
  - Lectures will not follow any textbooks
  - Lectures will focus on “big-picture” principles and ideas
- Attend sections (if you have questions about assignments, best to attend rather than watch later)
  - Details not covered in lecture, especially about homeworks and labs
  - More opportunity for discussion

# Guest Lectures

- We will have a few guest lectures throughout the quarter
  - Useful to give you a different perspective: e.g., research, industry, government, legal

# Course Logistics (CSE 484)

Security is a contact sport!

- Labs (45% of the grade)
- Homework (25% of grade)
- Participation and in-class activities (10% of the grade)
- Final project (20% of the grade)

# Course Logistics (CSE M 584)

Same as before, but...

- Labs (42% of the grade) [-3%]
- Homework (22% of grade) [-3%]
- **Research readings (10%)** [+10%]
- Participation and in-class activities (10%)
- Final project (16% of the grade) [-4%]

# Labs

- General plan:
  - 3 labs
    - First lab out next week (TBD)
  - Topics:
    - Software security (Buffer overflows, ...)
    - Web security (XSS attacks, SQL injections, ...)
    - Smart homes
  - Submit to Canvas
  - Groups must be configured *on Canvas*

# Homework

- 3 homeworks distributed across quarter
  - <http://courses.cs.washington.edu/courses/cse484/22au/assignments>
  - First homework out later today
- Do now (no later than October 3): sign ethics form!

# Ethics

- To learn to defend systems, you will learn to attack them. You must use this knowledge ethically.
- In order to get a non-zero grade in this course, you must electronically sign the “Security and Privacy Code of Ethics” form by 11:59pm on Monday, October 3.

(Linked from the course schedule)

*We will also repeatedly consider ethics (more generally) as part of our curriculum throughout course (see HW1, for example).*

# In-Class Participation

- Trying to bring the best of online to in-person
  - In-class discussions, polls, and other online tools
  - More use of the online discussion board
  - Questions live and via pollev
- **Main component: Lightly graded in-class activities**
  - Canvas “quiz” submission (intended for use during class, but can be submitted up until start of next lecture)
  - Not a “quiz” in the traditional sense



# Late Submission Policy

- 5 free late days, no questions asked
  - Cumulative, throughout the quarter
  - Use up to 3 for one submission
  - All group members use days at once
- After that, late assignments will be dropped 20% per calendar day.
  - Late days will be rounded up
  - So an assignment turned in 26 hours late will be downgraded 40%
  - See website for exceptions -- a small number of assignments must be turned in on time
- Please write on the assignment how many late days you are using!

# To Do

- Sign ethics form (due October 3)
  - <https://forms.gle/WMe1gQt26t5RAsY48>
- Homework #1 (due October 7)
  - Start forming groups (e.g., use discussion board) and thinking about technologies you'd like to review.

Questions?

[cse484-tas@cs.washington.edu](mailto:cse484-tas@cs.washington.edu)