CSE 484 / CSE M 584: Computer Security and Privacy

Autumn 2020

Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Hi!

- Instructor: Franziska Roesner (**Franzi**)
- TAs:

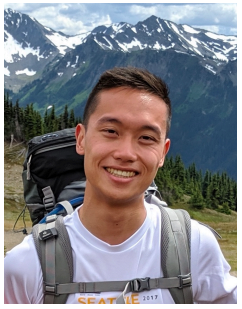
Wenqing Lan

Keanu Vestil

Erika Wolfe

Bowen Xu

Sherry Yang



Eric Zeng

Online Version 2.0

- We're disappointed we can't meet in person!
- I hope you are all doing okay
  - (It's okay if you're not)
- We learned a lot about running an online course in the spring, but this will still be a quarter of flexibility & patience
- **We are still excited to teach you about computer security and privacy!**
- Please let us know if something is not working for you, or if you need additional support

Online Course Plan

- Lectures and Sections and Office Hours via Zoom
  - Synchronous, but recorded*
    * Sections may be only partially recorded
    * Office hours will not be recorded
    * Recordings include student speech/video/chat (don't share if you don't want to!) and will not be shared outside the class
  - Access the links via Canvas
- Largely the same curriculum as usual
  - Labs and homeworks and final project; **no exams**
  - We will adapt throughout the quarter as needed

A Few Words About Zoom Chat

- Please **use it** to ask or answer direct questions
- Please **avoid** tangents or discussions
  - Have more thoughts? Things to share? Awesome! We want to hear them! Please use the discussion board, though.
- **Please be mindful of leaving space for others too**
- Rule of thumb: would you (or would you think someone should) say this out loud to everyone in a physical classroom?
- (We may experiment with other models throughout the quarter)

Course Resource Cheat Sheet

- **Zoom:** Lectures, sections, office hours
- **Canvas:** Links to Zoom events, assignment submissions, grades
- **Course website:** Schedule, assignment details, readings, policies
- **Ed:** Discussion board
- **Course mailing list:** Announcements
- **Email:** Reach course staff privately

What Does "Security" Mean to You?

Let's try a Zoom breakout!

- *What comes to mind when you think of computer security and privacy?*
- *What topics are you most excited about, or hoping we will cover this quarter?*

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
- Security deals with intentional failures created by intelligent parties
  - Security is about computing in the presence of an adversary
  - But security, reliability, and usability 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")
  - 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.

Two Key Themes of this Course

1. How to **think** about security
   - The "Security Mindset" – a "new" way to think about systems
2. **Technical aspects of security**
   - 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
- "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…"

- Why it's important
  - Technology changes, so learning to think like a security person is more important than learning specifics of today
  - 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 discussions and activities
  - Participation in Ed discussion board (e.g., critiquing movies)

A Word on Groupwork

- In some quarters, we require it
  - Need to learn how to work in groups
    - Especially if you don't like it ☺
  - Attack-based labs require some creativity, where group interactions can help generate ideas
- This quarter, with time zone and other challenges, we will be flexible as needed
- But, if you can, **we still encourage working in groups.** Social contact is important!
- (Please follow all the usual in-person contact guidelines ☺)

What This Course is Not About

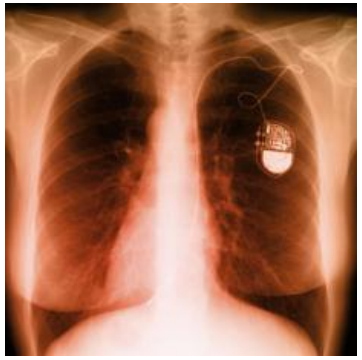
- Not a comprehensive course on computer security
  - Computer security is a broad discipline!
  - Impossible to cover everything in one quarter
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read news, discuss on forum
- Not a course on ethical, legal, or economic issues
  - We will touch on these issues, but the topic is huge
- Not a course on how to "hack" or "crack" 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

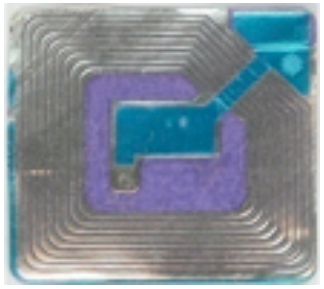
voting machines

EEG headsets



medical devices

wearables



RFID

mobile sensing platforms

cars

game platforms

airplanes

Communication

- franzi@cs.washington.edu
  - Use this if something is sensitive, confidential, etc.
- cse484-tas@cs.washington.edu
  - Use this to reach all course staff
- Ed Discussion Board
  - Use this if other students in the class would benefit from your question/answers **[common case]**
- Course mailing list: multi_csem584a_au20@uw.edu
  - We'll use this for announcements
- We will do our best to be responsive, but **please be professional**, and plan ahead!

Course Materials

- Readings:
  - Optional textbook: Daswani, Kern, Kesavan - "Foundations of Security"
  - Additional reading materials linked to from course website (sometimes **strongly recommended**)
- Attend lectures (or watch later)
  - Lectures will not follow the textbook and will cover a significant amount of material that is not in the textbook
  - Lectures will focus on "big-picture" principles and ideas
- Attend sections (or 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: 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 soon, likely next week
  - Topics:
    - Software security (Buffer overflows, …)
    - Web security (XSS attacks, SQL injections, …)
    - Smart homes
  - Submit to Canvas
  - Generally encourage groups

Homework

- 3 homeworks distributed across quarter
  - http://courses.cs.washington.edu/courses/cse484/20au/assignments.html
  - First homework out now (due October 9)

- Do now (no later than October 7): 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 Wed, Oct 7.

  (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

- Continuing to experiment with online course logistics
  - Zoom breakouts and polls
  - More use of the online discussion board
  - Questions live and via Zoom chat
  - Post-lecture surveys
- **Main component: Lightly graded in-class activities**
  - Usually involve a Zoom breakout
  - Canvas "quiz" submission (intended for use during class, but can be submitted up until start of next lecture)

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

To Do

- Ethics form (due Wed Oct 7 – do it now!)
- Homework #1 (due Fri Oct 9)
  - Now: Start forming groups (e.g., use discussion board) and thinking about technologies you'd like to review.

Questions?

franzi@cs.washington.edu

cse484-tas@cs.washington.edu