CSE 484 / CSE M 584: Computer Security and Privacy

Spring 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 ...

Welcome to the Strangest Quarter

- I'm disappointed we are not meeting in person!
- I hope you are all doing okay
  - (It's okay if you're not)
- This will be a quarter of flexibility and patience
- We are still excited to teach you about computer security and privacy!

Course Staff

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

Zetian Chen

Wenqing Lan

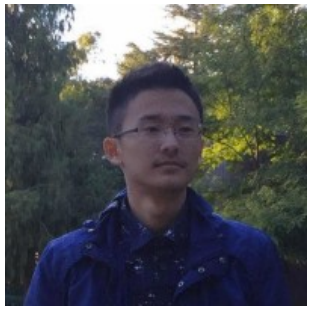
Patty Popp

Alex Teng

Erika Wolfe

Sam Wolfson

Bowen Xu



Jeff Zhao

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
  - Access the links via Canvas
- For now, we have planned roughly the same curriculum as usual
  - Labs and homeworks and final project; **no exams**
  - We will adapt throughout the quarter as needed

Using Zoom during Lecture

- Questions:
  - Please feel free to type questions into the chat
  - Zoom has a hand-raising feature, but I may not see it – you can also type "hand" into the chat
- Web cams:
  - We will not require you to turn it on (this is a privacy course after all…)
  - But if you're comfortable, video can help us feel more connected

Course Access Survey

Please fill this out to help me understand potential challenges with accessing the course (e.g., technology, time zones):

https://forms.gle/sY4b19cFaEKrq0Qp6

What's Wrong With This Picture?

What's Wrong With This Picture?

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
- We will do our best to be responsive, but **please be professional**, and plan ahead!

Mailing List

multi_csem584a_sp20@uw.edu

- Make sure you're on the mailing list
  - You should have already received emails
  - If you recently enrolled, wait 24 hours
- URL for mailing list on course website
- We will use the mailing list for **announcements**; please use the Ed Discussion Board for discussions

Quiz Sections and Office Hours

- Quiz sections on **Thursdays:**
  - 12:30-1:20pm
  - 1:30-2:20pm
  - 2:30-3:20pm
  - 3:30-4:20pm
- Office hours
  - Franzi: 11:30am-12:30pm Mondays
  - TAs: To be announced for next week
- Zoom links on Canvas

Prerequisites (CSE 484)

- Required: Data Abstractions (CSE 332)
- Required: Hardware/Software Interface (CSE 351)
- Assume: Working knowledge of C and assembly
  - One of the labs will involve writing buffer overflow attacks in C
  - You must have detailed understanding of x86 architecture, stack layout, calling conventions, etc.
- Assume: Working knowledge of software engineering tools for Unix environments (gdb, etc)
- Assume: Working knowledge of Java and JavaScript
- **Assume: Ability to learn new programming languages / skills easily**

Prerequisites (CSE 484)

- Useful (not required): Computer Networks; Operating Systems
  - Will help provide deeper understanding of security mechanisms and where they fit in the big picture
- Useful (not required): Complexity Theory; Discrete Math; Algorithms
  - Will help with the more theoretical aspects of this course.

Prerequisites (CSE 484)

- Most of all: Eagerness to learn!
  - This is a 400 level course.
  - We expect you to push yourself to learn as much as possible.
  - We expect you to be a strong, independent learner capable of learning new concepts from the lectures, the readings, and on your own.
  - **Of course, this quarter is different than usual. Take care of yourselves and communicate with us!**

Course Materials

- Textbook (suggested):
  - Daswani, Kern, Kesavan, "Foundations of Security"
  - Additional materials linked to from course website
- 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)
  - Hands-on experience with security issues
- Homework (25% of grade)
- Participation (10% of the grade)
  - More details later
- 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 (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

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 strongly encourage working in groups.** Social contact is important!

Homework

- 2 or 3 homeworks distributed across quarter
  - http://courses.cs.washington.edu/courses/cse484/20sp/assignments.html
  - First homework out now (due April 10)

- Do now (no later than April 8): 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, April 8.

(Linked from the course schedule)

Final Project

- **No midterm or final exam!**
- Instead: **12-15 min video** about a security/privacy topic of your choice
  - Groups of up to 3 people
  - Security is a broad field, and this class can't remotely cover everything – this is your chance to explore a security or privacy topic in more detail!
  - Multiple checkpoint deadlines throughout quarter
- Details linked from website's Assignments page

Participation

- Still figuring out how to best do this in an online course
  - Zoom breakouts and polls
  - More use of the online discussion board
  - Questions live and via Zoom chat
  - Post-lecture surveys
- Unlike past quarters, in-class activities (previously worksheets) **will not** contribute to your grade
  - But we'd still like to see participation in the chat, office hours, section, discussion board, etc.
  - Ideally throughout the quarter, not 10 posts on the last day of class
  - We will be flexible

Discussion Board

- We've set up a Ed Discussion Board for this course:
  - https://us.edstem.org/courses/414/discussion/
- Please feel free to post to Introductions thread now
- Please use it to discuss the homework assignments and labs and other general class materials
- You can also use it to exercise the "security mindset"
  - Discussions of how movies get security right or wrong
  - Discussions of news articles about security (or not about security, but that miss important security-related things)
  - Discussions about security flaws you observe in the real world

Late Submission Policy

- 3 free late days, no questions asked
  - Cumulative, throughout the quarter
  - Use however you wish (all at once, 3x1, …)
  - 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 -- some assignments must be turned in on time

What Does "Security" Mean to You?

Let's try a Zoom breakout!

What comes to mind when you think of computer security and privacy?

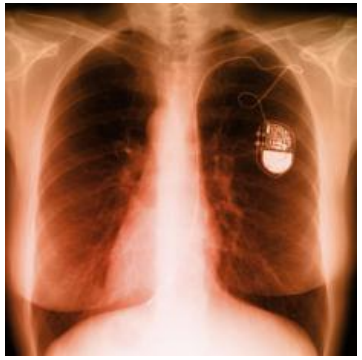
What topics are you most excited about, or hoping we will cover this quarter?

Security: Not Just for PCs

smartphones

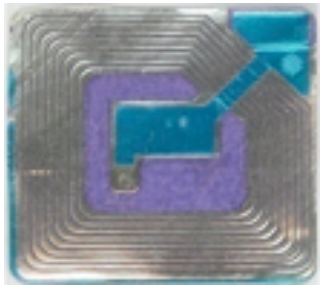
voting machines

EEG headsets



medical devices

wearables



RFID

mobile sensing platforms

cars

game platforms

airplanes

To Do

- Ethics form (due Wed April 8 – do it now!)
- Homework #1 (due Fri April 10)
  - Now: Start forming groups (e.g., use discussion board) and thinking about events and technologies you'd like to review.

Questions?

franzi@cs.washington.edu

cse484-tas@cs.washington.edu