CSE 484 / CSE M 584: Computer Security and Privacy

Spring 2024

David Kohlbrenner
dkohlbre@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: David Kohlbrenner (he/him)

TA Staff

- **Sara Deutscher**
- **Joo Gyeong Kim**
- **Navkiran Nijjar**
- **Lin Qiu**
- **Basia Radka**
- **Deepayan Sanyal**
- **William Travis**
- **Anna Wang**
- **Shaoqi Wang**

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 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
- Evaluation
  - Labs
  - Homeworks
  - Final project; **no exams**
  - Participation/in-class exercises

Course Resource Cheat Sheet

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

Pollev and Canvas

- We'll do a lot of breakouts in class
- Depending on the topic, we'll be using pollev or canvas

https://pollev.com/dkohlbre today

What Does “Security” Mean to You?

1) Spend a few minutes defining security in the context of computing/technology.

Try putting some answers in https://pollev.com/dkohlbre

What Does “Security” Mean to You?

1) Spend a few minutes defining security in the context of computing/technology.
2) Talk to your neighbors about your definitions
3) Come up with a group definition

Try putting some answers in https://pollev.com/dkohlbre

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

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 2 people (groups are encouraged – **lots of value in discussing security with others!**)
  - In class discussions and activities
  - Participation in Ed discussion board (e.g., asking about news stories, technologies)

A Word on Groupwork

- 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

- Make sure everyone works on _all_ parts of the labs/HWs
  - Don't split up problems and assign them out!

*contact course staff ASAP if this isn't going to work for you

What This Course is Not About

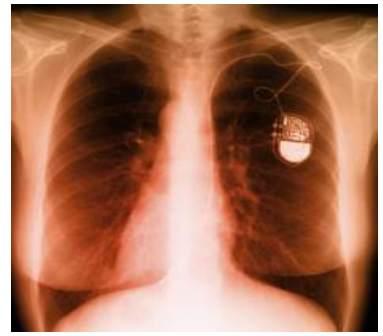
- Not a comprehensive course on computer security
  - Computer security is a broad discipline!
  - Impossible to cover everything in one quarter
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read news, ask questions, discuss on Ed
- Not a course 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

- dkohlbre@cs
  - Use this if something is sensitive, personal, confidential, etc.
- cse484-tas@cs.washington.edu
  - Use this 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]**
- We will do our best to be responsive, but **please be professional**, and plan ahead!

Course Materials

- Readings:
  - I'll be posting reading materials as we go
  - Feel like we're missing something? Let me know!
- 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: 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!
  - Topics:
    - Software security (Buffer overflows, …)
    - Web security (XSS attacks, SQL injections, …)
    - Finding + fixing vulnerabilities
  - Submit to Canvas/gradescope
  - Groups must be configured *on Canvas*

Homework

- 3 homeworks distributed across quarter
  - First homework out shortly

Ethics

- To learn to defend systems, you will learn to attack them. You must use this knowledge ethically.

In-Class Participation

- Trying to bring the best of online, 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
  - Don’t ask us about more late days, use these _first_
- 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

Discussion Board

- We've set up a Ed Discussion Board for this course
- 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

Generative AI Tools (aka ChatGPT)

- Tl;dr: We heavily discourage using these tools in 484
  - You may *not* use them to solve assignments/questions
  - You may (with disclosure) ask basic factual questions related to 484
  - See course webpage for full policy

Announcements

- We will use Ed for **announcements**
  - It will send an email to you for announcements

Final Project

- **No midterm or final exam!**
- Final project will require you to find and fix vulnerabilities in a medium (~1200 lines) piece of software.
  - Lab 3 will be warmup for the final project
- You will also need to explain your decisions and evaluation of the vulnerabilities
  - This will be either scheduled with TAs or a video (TBD)

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 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.

Discussion

- **Everyone** in this class **deserves** to be in this class!!
- We are **all** coming to this course with **different backgrounds** and experiences
- There are **no bad questions**; never belittle a questioner or their question; always be supportive
- Instructors / staff aren't always aware of everything, so **please call our attention to things as needed**
  - E.g., someone might harm someone else with what they say without ever realizing that what they said is harmful; that harm still exists, regardless of whether there was an intent to harm

Another Example

To Do

- Homework #1
  - Now: Start forming groups (e.g., use discussion board) and thinking about technologies you'd like to review.

Questions?

dkohlbre@cs

cse484-tas@cs.washington.edu