CSE 484/M584: Computer Security (and Privacy)

Spring 2025

David Kohlbrenner
dkohlbre@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner, Nirvan Tyagi. 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

- Micah Chang
- Pranati Dani
- Gregor Haas
- Jasmine Herri
- Evan Lam
- Sela Navot
- Rasmus Makiniemi
- Hoang Nguyen
- Shreya Sathyanarayanan

Course Plan

- Lectures: in-person
  - Lectures are recorded to Panopto (please attend!)
    * Recordings include student speech/video/chat and will not be shared outside the class
- Office hours:
  - TBD, announced today or tomorrow.
- Evaluation
  - 4 Labs
  - 1-2 Homeworks
  - Participation/in-class exercises
  - **Final exam** (June 9th)

Course Resource Cheat Sheet

- **Course website:** Schedule, assignment details, readings, policies
- **Panopto:** Lecture recordings
- **Ed:** Discussion board, Announcements
- **Gradescope:** Assignment handin + grades
- **Email:** Reach course staff privately

Gradescope In-class activities

- We'll do a lot of breakouts in class

- Breakouts are four parts:
  - Think (solo)
  - Pair (discuss with neighbors)
  - Writeup (Summarize your discussion on Gradescope)
  - Share (Full-class discussion)

What Does “Security” Mean to You?

1) Spend a minute defining security in the context of computing/technology to yourself.
2) Discuss with your neighbors.
3) Think of a computer security practice you do/want to do.
4) Summarize on Gradescope
5) Share!

Try putting some answers in Gradescope.

Why 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

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

Lea Kissner 
@LeaKissner

I was just asked what the differences are between the fields of privacy, security, and health/trust&safety. Here's my best shot -- do you have better?

Security: our products/systems behave how they're supposed to, even in the presence of adversaries

10:37 AM · Sep 14, 2022 · Twitter for Android

Lea Kissner 
@LeaKissner

Privacy: our products/systems behave respectfully towards the people who use and are affected by them

T&S: users interact respectfully with each other through our products/systems

10:37 AM · Sep 14, 2022 · Twitter for Android

https://twitter.com/LeaKissner/status/1570104506477867008

Two Key Themes of this Course

1. How to **think** about security and privacy
   - The "Security Mindset"
   - (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 range widely, tell us if something you'd like isn't covered

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; 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
  - Reading papers!
  - In class discussions and activities
  - Labs
  - Participation in Ed discussion board (e.g., asking about news stories, technologies)

What This Course is Not About

- Not a comprehensive course on computer security
  - Impossible to cover everything in one quarter
- 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

Communication

- dkohlbre@cs.washington.edu
  - 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
  - Default platform for questions, supports private and public posts.
  - Also announcements
- We will do our best to be responsive, but please be professional, and plan ahead!

Course Materials

- Lectures
  - Lectures are where the bulk of information is
  - Lectures are interactive, and have discussion periods
  - Please attend!

- There will be optional readings posted for most classes
  - These may be *very* helpful for assignments
  - Or simply relevant and interesting

Guest Lectures

- We may have some guest lectures during the quarter
  - They will be announced ahead of time if we're having one

Course webpage

Grading, labs, etc.

Ethical security work

- We’re going to discuss how to break things
  - Please be responsible with this knowledge
  - Understanding flaws is critical to fixing them

In-Class Participation

- **Main component: Lightly graded in-class activities**
  - Gradescope submission, effort not correctness

Late Submission Policy

- 5 free late days, no questions asked
  - Cumulative, throughout the quarter
  - Use up to 3 for one submission
  - Don’t ask us about more late days, use these _first_
- Otherwise, assignments will be dropped 20% per calendar day.
  - Late days will be rounded up
  - 26 hours late is 2 days (40% deduction)

Discussion Board

- We've set up a Ed Discussion Board for this course
- Please use it to discuss 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

Announcements

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

Academic Integrity

- You will only learn effectively if you complete the intellectual work of this course.
  - This is not the same as completing the *work* of the course.

- Acceptable collaboration examples:
  - Asking a friend about the mechanics of different C string functions.
  - Discussing which references you found useful for a given part of a lab.
  - Helping someone trouble-shoot SSHing into course servers.
  - Discussing an example from class, and how you might adapt it to other problems (assuming that other problem is not in a homework/lab.)

- If you are found to violate course policies 2 or more times, you may receive a 0 in the course.

Generative AI Tools (aka ChatGPT)

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

- Our experience has been that GenAI solutions to security problems are *particularly bad*
  - This is backed up by studies (so far) on the security quality of GenAI code

- Not disclosing GenAI use is an academic integrity violation.

Labs

- **Lab 1 goes out this week**
  - Binary exploitation (remember your 351 bomblab?)
- Lab2: Cryptography lab
  - New lab this quarter
  - Several short cryptography problems in Python
- Lab3: Web lab
  - Basics of web application exploitation
- Lab4: RCA (Root Cause Analysis) lab
  - Evaluate the security of a small C application
  - Patch security vulnerabilities

Final Exam

We have a final exam this quarter. On paper, in-person.

It will draw on the labs and lectures.

June 9th 8:30am

10% of the course grade

CSE M584

- Weekly research readings + Summaries
- You will need to submit 1 paper summary each week, due Friday at 11:59pm.
  - That includes this week!
- See the course webpage for more information.

Prerequisites (CSE 484)

- Assume: Working knowledge of C and assembly
  - One of the labs will involve writing buffer overflow attacks in C
  - You will need a 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**

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

Threat Modeling