CSE 484 / CSE M 584: Computer Security and Privacy

Fall 2023

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: Franzi (Prof. Franziska Roesner) (she/her)
- TA Staff:
  - Sara Deutscher
  - Sonia Fereidooni
  - Kirsten Graham
  - Akash Gujjar
  - Evan Lam
  - Lin Qiu
  - Basia Radka
  - Shaoqi Wang

Course Resource Cheat Sheet

- **Course website:** Schedule, assignment details, readings, policies
- **In Person:** Lectures, sections, office hours
- **Zoom:** Limited office hours
- **Canvas:** Links to recordings, assignment submissions, grades
- **Ed:** For official announcements and discussion
- **Gradescope:** Some assignments
- **Email:** Reach course staff privately (cse484-tas@cs)

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.
4. 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

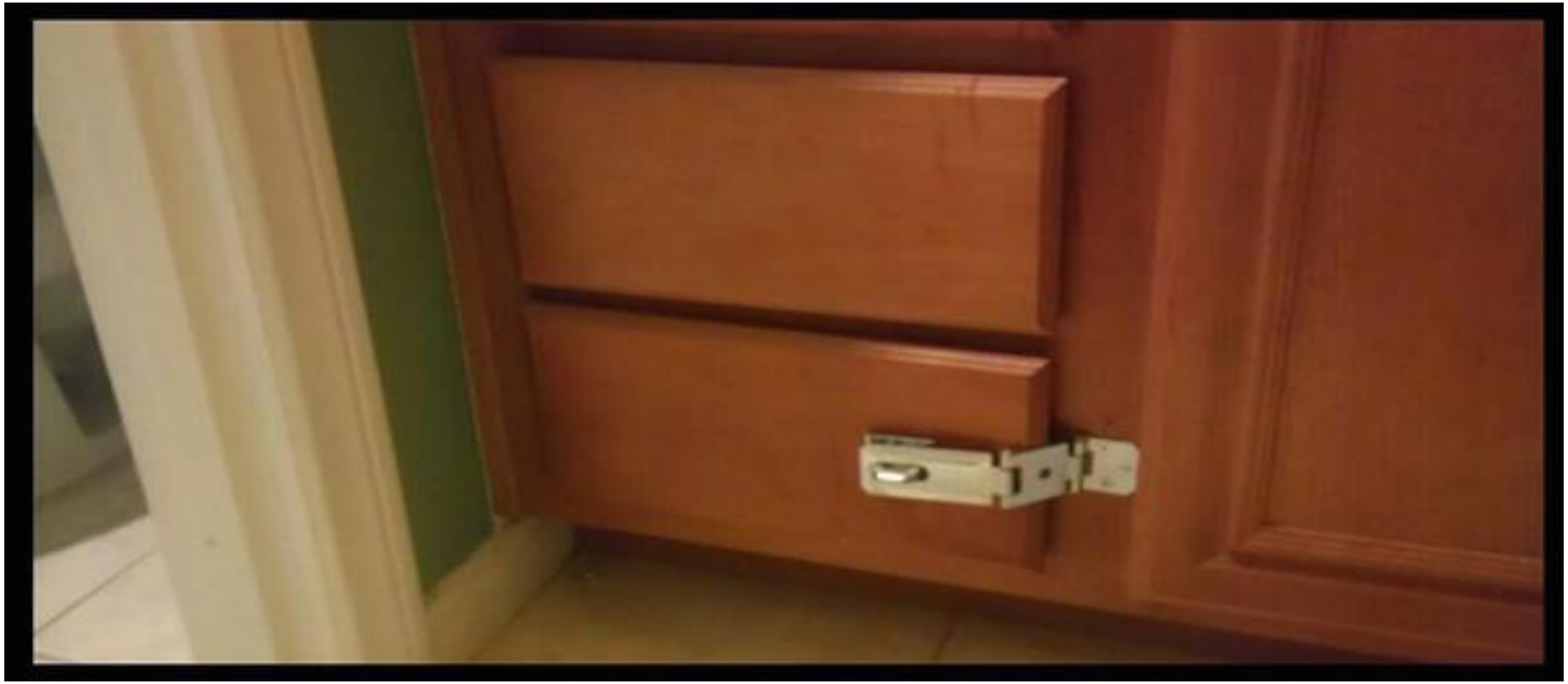
Two Key Themes of this Course

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

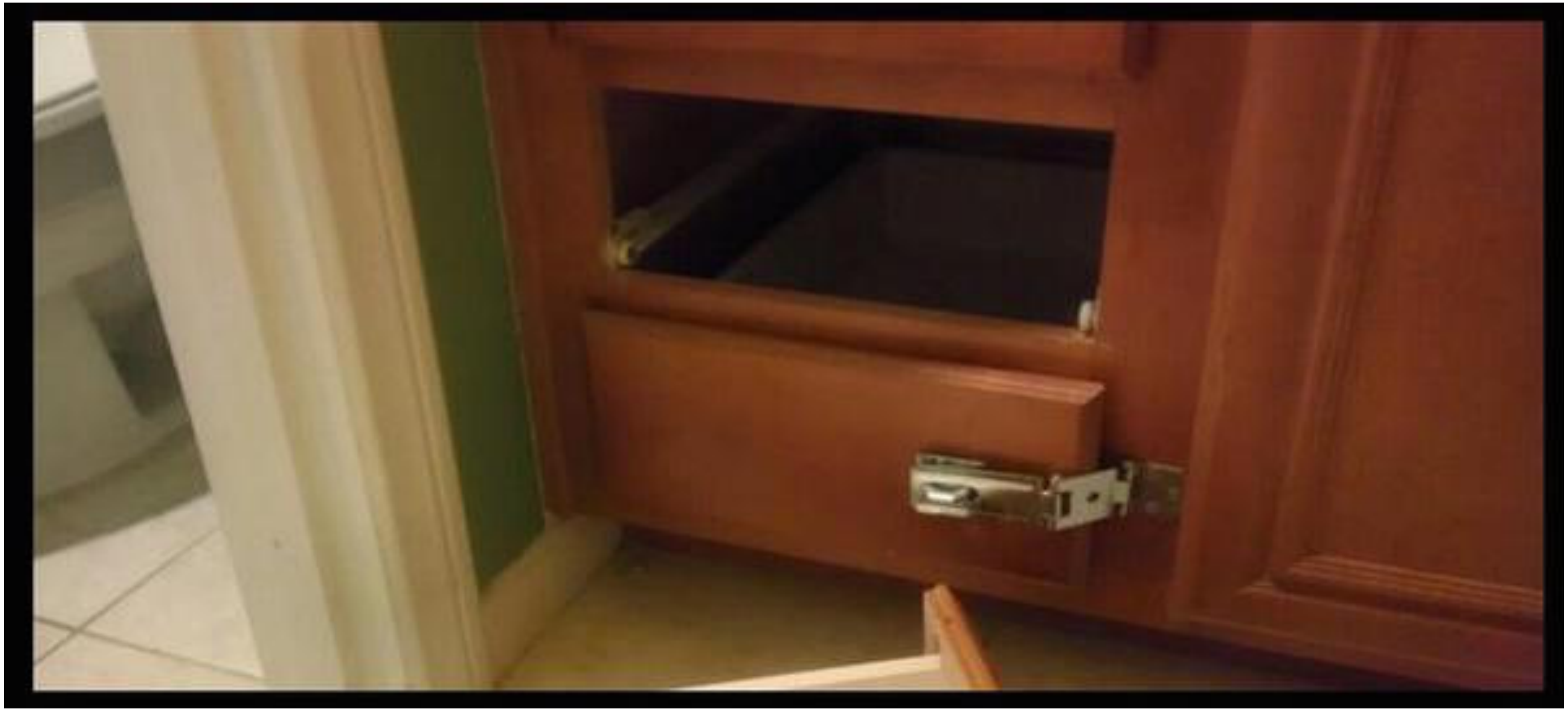
Theme 1: Security Mindset

- 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)

Security: Not Just for PCs

smartphones

wearables

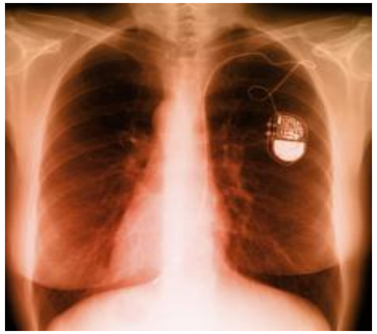
voting machines

RFID

game platforms

EEG headsets

mobile sensing platforms


medical devices

cars

airplanes

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

Communication

- franzi@cs
  - Use this (or instructor office hours) if something is sensitive, personal, confidential, etc.
- cse484-tas@cs.washington.edu
  - Best method to reach all course staff (including instructor) for admin issues
- 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:
  - No textbook; I’ll be posting reading materials as we go
  - Some optional, some **strongly recommended**
- Attend lectures
  - Lectures are recorded (but 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
- Attend sections
  - 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 (40% of the grade) [-5%]
- Homework (20% of grade) [-5%]
- **Research readings (10%)** **[+10%]**
- Participation and in-class activities (10%)
- Final project (20% of the grade)

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
  - **Groups must be configured *on Canvas***

Labs

- General plan:
  - 3 labs
    - First lab out next week (TBD)
  - Topics:
    - Software security (Buffer overflows, …)
    - Web security (XSS attacks, SQL injections, …)
    - Vulnerability patching
  - Submit to Canvas
  - You might find unintended vulnerabilities in the labs! ☺ We expect you to responsibly disclose these, rather than exploiting them.

Homework

- 3 homeworks distributed across quarter
  - http://courses.cs.washington.edu/courses/cse484/23au/assignments
  - First homework out now!

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

Final Project

- **No midterm or final exam!**
- There will be a final project, likely extending Lab 3

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 2.

(Linked from the course schedule)

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

Late Submission Policy

- 5 free late days, no questions asked
  - Cumulative, throughout the quarter
  - All group members use days at once
  - **Intended to give you flexibility, not for you to hoard them ☺**
- 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 few assignments must be turned in on time
- **Please write on the assignment how many late days you are using!**

ChatGPT?

- ChatGPT and related tools are useful, but have risks: providing incorrect information, simply copying text from other sources, undermining learning goals of an assignment in which we are asking you to think critically.
- In this class:
  - (1) Whether you use generative AI or read someone's blog post or code, you are expected to ensure that the final product is your own, original work.
  - (2) Though we discourage it, you may use generative AI unless specified otherwise for an assignment, but you must disclose what tool you used, as well as provide the prompts you used.
  - (3) You are responsible for ensuring that the resulting text is correct, that any included ideas are properly cited, and that there is no text plagiarized from other sources.
  - (4) Please note that using such tools may imply donating your data to companies.
- Finally, note that if the results are that your writing is narrower and shallower in scope this may impact your grade.

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 (or develop) 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.
  - **It is okay and expected if you are not able to get every possible point.**
  - **At the same time: Take care of yourselves and communicate with us!**

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

To Do

- Sign ethics form (due October 2)
- Homework #1 (due October 6)
  - 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