CSE 484 / CSE M 584: Computer Security and Privacy

Spring 2021

Tadayoshi Kohno (Yoshi)
yoshi@cs

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

Hello ☺

- Instructor: Tadayoshi Kohno (he/him)
- TAs:
  - Donna Albee
  - Jeter Arellano
  - Arka Bhattacharya
  - David Chen
  - Ivan Evtimov
  - Wenqing Lan
  - LuLu Pinczower
  - Jeffery Tian
  - Bowen Xu
  - Sherry Yang

Online, again

- We're disappointed we can't meet in person!
- I hope you are all doing okay
  - If you're not, that is normal, but please make sure to seek help where needed, talk with the advisors, talk with others, talk with us
- While we've been running classes online for some time, things won't be perfect
- **We are still excited to help you learn about computer security and privacy!**
- If something about the course isn't working, let us know! The sooner you do, the better

Online Course Plan

- Lectures and Sections and Office Hours via Zoom
  - Synchronous, but 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
- 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**

More About Zoom Chat, Breakout Rooms, and in General

- **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

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 (though most go to Ed)
- **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?*

There are no right or wrong answers!


information assurance
securing account password
Buffer Overflow
preemptive planning
spectre/meltdown
leaks
Social Engineering
private data
Phishing
DDOS
security breaches
scandals
protecting data
hackers
exploit
Encoding
protecc
protect
hacker
safety
viruses
social media
data
Hashing
personal
necessary
encryption
HTTPS
hacking
cryptography
Breaches
Network
Vulnerabilities
passwords
Protection
Alexa
paswords
Privacy
virus
password
leak
Antivirus
salt
information
smart devices
misinterpretation
injection
Exploitation
unintended code behavior
senstive information

What are topics you are excited about?

- It is also okay if you don't know what topics you are interested in yet!
- We can ask this question again at the end of the course, after you know more about different topics.


determining how to prepar
authentification
securing websites
social engineering
end-to-end encryption
captcha
everything?
phishing
differential privacy
protection
Ethics
images
personal security
bugs
Web security
data security
blockchainn
virus
ethical hacking
rsa
password storage
exploits
hacking
Unsure
hashing
data storage
encryption
data ethics
xss
cryptography
Not sure
privesc
injection
history of security
buffer overflow
networks
fun exploits
facial recognition
don't know yet
blockchain
Network Security
hack
bad security
privacy
security
passwords
facebook
unethical hacking
privacy and government
personal health data

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 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., asking about news stories, technologies)

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 strongly, strongly discourage singleton groups
- To repeat, if you can, **we still encourage working in groups.**
  - Social contact is important!
  - Lab 1 is *very* hard without a group; the learning through group discussion for Homework 1 is valuable, …
- (Please follow all the usual in-person contact guidelines ☺)

What This Course is Not About

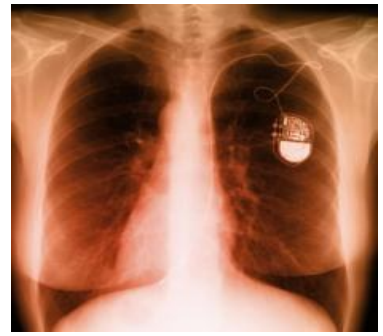
- Not a comprehensive course on computer security
  - Computer security is a broad discipline!
  - Impossible to cover everything in one quarter
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read news, ask questions, discuss on Ed
- Not a course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

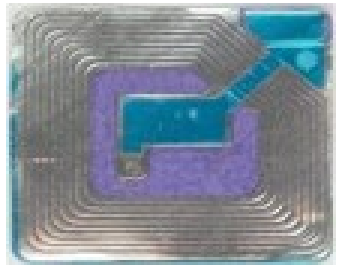
voting machines

EEG headsets



medical devices

wearables



RFID

mobile sensing platforms

cars

game platforms

airplanes

Communication

- yoshi@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]**
- Course mailing list: multi_cse484a_sp21@uw.edu
  - We'll use this (and Ed) 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"
    - Really, the textbook is optional; it was cutting edge at the time it was written; now, it is still a great resource for learning how to think about security and for learning some key background concepts, but it is not current
  - 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 (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, likely next week
  - Topics:
    - Software security (Buffer overflows, …)
    - Web security (XSS attacks, SQL injections, …)
    - Smart homes
  - Submit to Canvas
  - Groups highly encouraged unless stated otherwise

Homework

- 3 homeworks distributed across quarter
  - http://courses.cs.washington.edu/courses/cse484/21sp/assignments
  - First homework out TBD (due April 7)

- Do now (no later than April 5): sign ethics form! (See course Administrivia Page)

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 April 5, 2021.

  (Linked from the course administrivia page, under Ethics Form)

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, polls, and other online tools
  - More use of the online discussion board
  - Questions live and via Zoom chat
- **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); *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
- 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

Mailing List

multi_cse484a_sp21@uw.edu

- Make sure you're on the mailing list
  - We'll send an email later today
  - If you recently enrolled, wait 24 hours
- URL for mailing list on course website
- We will use the mailing list and/or Ed for **announcements**; please use the Ed Discussion Board for discussions (not the mailing list)

Discussion Board

- We've set up a Ed Discussion Board for this course:
  - https://edstem.org/us/courses/4935/discussion/
- 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

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

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!**

Another Example

To Do

- Ethics form (due April 5 – do it now!)
- Homework #1 (due April 7)
  - Now: Start forming groups (e.g., use discussion board) and thinking about technologies you'd like to review.

Questions?

yoshi@cs

cse484-tas@cs.washington.edu