CSE 564:
Graduate Computer Security and Privacy

Winter 2025

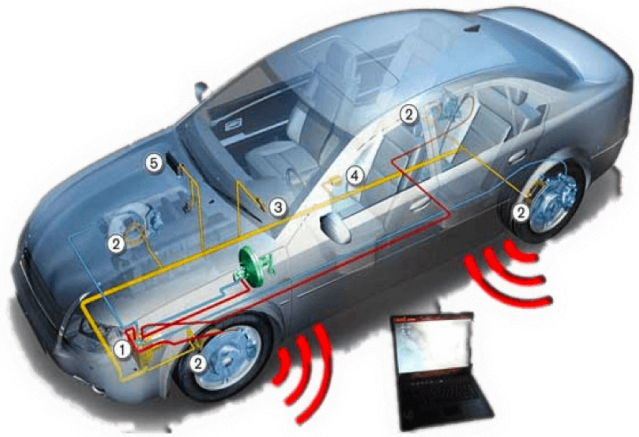
Tadayoshi (Yoshi) Kohno
yoshi@cs

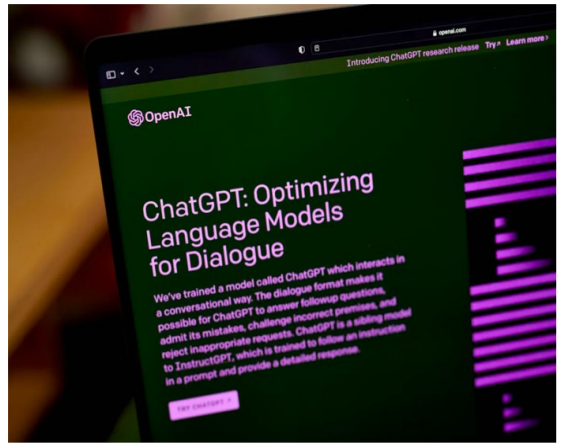
UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner.

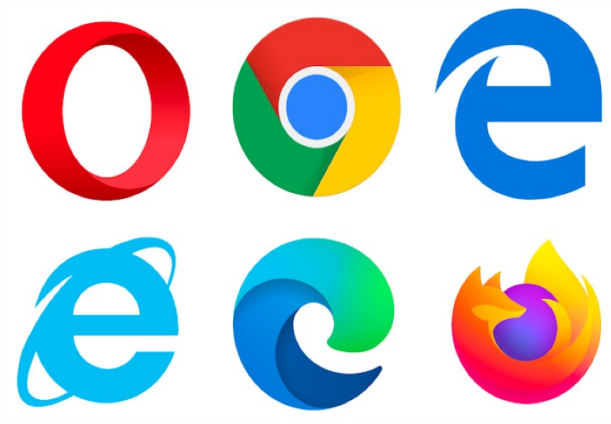
Hello ☺

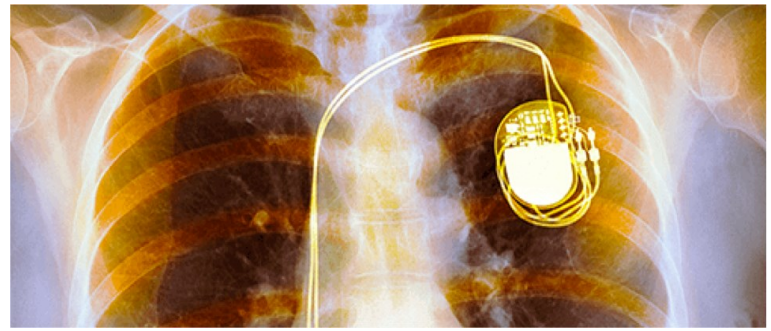
- Instructor: Yoshi Kohno
- TA: Rachel McAmis

New technologies bring new benefits…









…but also new risks!

Computer Security

- **Computer security:** A field focused on computing in the presence of adversaries
  - Victims of the adversaries could be using computers
  - Adversaries could be using computers
  - Both of the above
- **Privacy:** Much harder to define
  - Outside of the security community: Do system designs support privacy
  - Inside the security community: The above *and* can an adversary manipulate the system to access even more information

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

What is "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

Computer Security & Privacy Research

- **High-level goal:** Understand and protect stakeholders from adversarial security & privacy risks with existing and emerging technologies.
- **Broad technical focus:** A "lens" through which to view the rest of computer science (and beyond)!
- **Variety of methods / "ways of knowing":**
  - Analysis / Attacks
  - Measurement
  - Studying people
  - System design / building

This Course

- **High-level goal:** Introduction to and immersion in computer security & privacy research
- **More specific goals:**
  - Teach or sharpen a **security mindset** (challenge assumptions, think critically)
  - Introduce a **broad range of security & privacy topics**, and bring you to the forefront of research on those topics
  - Ultimately, **design more secure & private systems**
  - Provide **background & perspective** for your research – in security or otherwise!
- **Non-goal:**
  - Learn any specific security/privacy technologies. This course is complementary to an undergrad security course (like CSE 484).

Why I Like Security & Privacy Research

- **Breadth of topics** to explore: Issues wherever there is computation
- **Breadth of methods** to one can apply
- Focuses on the interplay between **technology and society**
- **Fun** – and challenging! – to think like an adversary

Introduction

- **On notecards, please write down your:**
  - Name (*)
  - Pronouns (*)
  - Program + Year in program
  - Research area(s) or subdisciplines/fields that interest you the most (*)
  - Prior experience with security and/or privacy (none is okay!)
  - What brings you to this course
  - Anything else you'd like me to know
- Toward the end of class, we will go around the room and introduce ourselves to each other – at least all the blue (*) bullets

Course Structure and Expectations

- Research readings and discussions
  - Reading papers
  - Writing responses
  - Participating in class
- Group-based research project
  - Checkpoints throughout the quarter
- Security reviews

Course Structure and Expectations

- Two meetings per week: M/W 11:30am-12:50pm
- **Research and discussion focused course**
  - Mainly **discussions of papers** (2 per class)
    - A couple of people to lead the discussion for each class (~TBDx per quarter), but everyone should come prepared to discuss the assigned papers
    - Participation counts for a non-negligible portion of your grade
  - **Class is in-person only!** If you need to miss, let me know. We expect that people may need to miss sometimes for illness, conference, etc., but expect you at a large majority of discussions. **Talk to us about your needs!**

Evaluation

- 45%: Research Project
- 10%: Project Workshopping
- 35%: Assignments
  - Discussion board posts
  - Discussion leading
  - Security reviews
- 10%: Class Participation

Class Participation

- An important part of your grade
- Because:
  - We would like you to read and think about papers throughout the quarter
  - **Important to learn to discuss papers**
- Expectations:
  - Ask questions, raise issues, think critically
  - Learn to express your opinion
  - **Respect and invite other people's opinions**
  - While thinking critically, also look for the value in papers

More on Discussions (Spoken, Written)

- We are all coming to this course with different backgrounds and experiences
- There are no bad comments; never belittle anyone or their comment; 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

Reading Writeups

- Due at 9am before every class
  - You have 4 "freebies" (but remember that there are 2 per class)
- Short: one paragraph per paper (2 paragraphs total)
- Say something that *hasn't been said yet*
- Examples:
  - Paper summary, key points
  - Evaluation, opinions, response to others' opinions (being thoughtful/mindful/courteous)
  - Questions for discussion, responses to others' questions
  - Open research questions
  - Broader implications, relationships with previous papers or your own research
- Graded on scale of 0-2

Reading + Writeup + Discussion Goal

- Goal with the writeups is to have an opportunity for thoughtful reflection
- That reflection *is* part of the learning process
- So, please don't use ChatGPT to generate your writeups

- Also: Okay (and important) to critique papers, but also consider: why was this paper accepted?

Expectations for Reading Papers

- You will likely not understand everything in every paper!
  - That is okay and expected! The field is so broad!
  - It is a useful skill to learn to get value from the papers anyway
- How long should you spend reading a paper?
  - 1-2 hours for reading + response, max
  - You will get faster as you go

Sample Topics (Unordered)

- Authentication
- Usable Security
- Side Channels
- Systems Security
- Web Security and Privacy
- Applied Cryptography
- Emerging Technologies
- Marginalized & Vulnerable Populations
- Anonymity
- Security + AI
- Misinformation
- …

Computer Security Publication Venues

- USENIX Security
- IEEE Symposium on Security & Privacy (aka “Oakland” or S&P)
- ACM Computer and Communications Security (CCS)
- Network and Distributed Systems Symposium (NDSS)
- Symposium on Usable Privacy and Security (SOUPS)
- Privacy Enhancing Technologies Symposium (PETS)
- European Symposium on Security & Privacy (EuroS&P)
- …
- Also papers/tracks in other fields’ core venues, e.g., CHI, WebConf

Security Reviews Assignment (2)

- Goal: learn to evaluate potential security and/or privacy issues with new technologies
  - For example, something you see in the news, on social media, in stores, etc.
- 2-3 pages, submit to Gradescope/Canvas
- You may work individually or (preferably) in groups of 2-3
- Follow specific format on website

Research Project

- Groups of 2-4 people (talk to me for exceptions).
- Topic:
  - Choose from a list of topics, or come up with your own.
  - Can be related to your ongoing research.
  - Can be related to a project in another course.
  - Must be related to computer security and/or privacy.
  - I encourage you to come talk to me about ideas.
- Types of projects: **Design/Build**, **Analyze**, **Measure**, **Human Aspects**
- Strive for **rigorous science**, though at a smaller scale than a full publication

Research Project

- Final deliverable:
  - Conference-style report (at most 12 pages) and presentation
- Milestones (see course website for deadlines)
  - Group formation
  - Project proposal
  - Checkpoint
  - Draft
  - Presentation (March 18 and 19)
  - Final report
  - Summary of contributions
- If your group isn't working out, contact me ASAP

Introduction (Revisited)

- **On notecards, please write down your:**
  - Name (*)
  - Pronouns (*)
  - Program + Year in program
  - Research area(s) or subdisciplines/fields that interest you the most (*)
  - Prior experience with security (none is okay!)
  - What brings you to this course
  - Anything else you'd like me to know
- Toward the end of class, we will go around the room and introduce ourselves to each other – at least all the blue (*) bullets

Today's Discussion (As Time Allows)

- Find a new person to talk to (2x) and discuss one or both of:
  - (1) Thinking about your own current research (if any), what are some security, privacy, or safety considerations?
  - (2) What security, privacy, or safety topics are on your mind due to current events, emerging technologies, or otherwise?