CSE 564:
Graduate Computer Security and Privacy

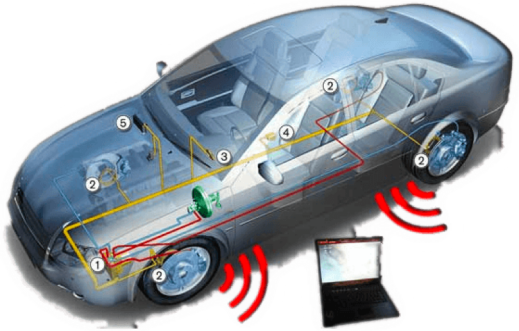
SECURITY & PRIVACY
RESEARCH LAB
UNIVERSITY of WASHINGTON

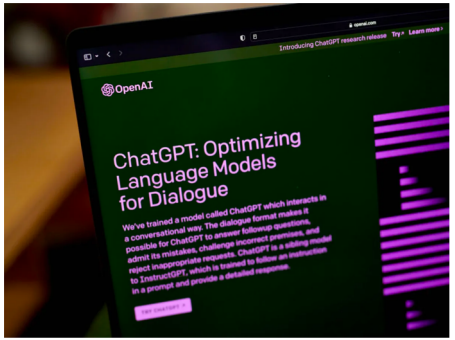
PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

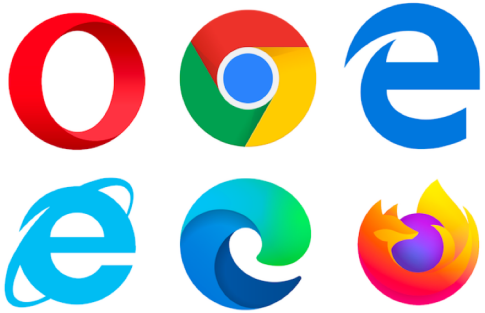
Course Staff

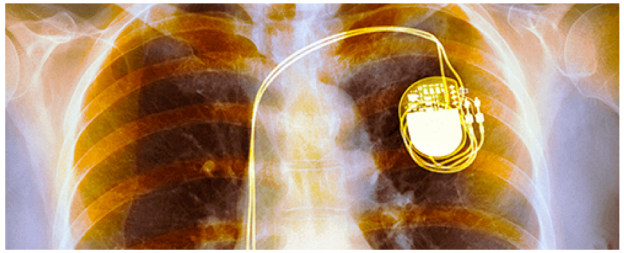
- Instructor: **Franzi Roesner** (franzi@cs.washington.edu)
  - Office hours Fridays 10:30-11:30am, CSE2 314
- TA: **Kentrell Owens** (kentrell@cs.washington.edu)
  - Office hours by appointment

New technologies bring new benefits…









… but also new risks.

Computer Security & Privacy Research

- **High-level goal:** Understand and protect computer security and privacy in 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

For Example…

Re: CAPTCHAs – Understanding CAPTCHA-Solving Services in an Economic Context

Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon McCoy,
Geoffrey M. Voelker and Stefan Savage
University of California, San Diego
{mmotoyam, klevchen, ckanich, dlmccoy, voelker, savage}@cs.u

Computer Security and Privacy for Refugees in the United States

Lucy Simko*, Ada Lerner†, Samia Ibtasam*, Franziska Roesner* and Tadayoshi Kohno*
*Paul G. Allen School of Computer Science & Engineering
University of Washington, Seattle, WA 98195
†Wellesley College
Wellesley, MA 02481

Spectre Attacks: Exploiting Speculative Execution

Paul Kocher[1], Jann Horn[2], Anders Fogh[3], Daniel Genkin[4],
Daniel Gruss[5], Werner Haas[6], Mike Hamburg[7], Moritz Lipp[5],
Stefan Mangard[5], Thomas Prescher[6], Michael Schwarz[5], Yuval Yarom[8]
[1] Independent (www.paulkocher.com), [2] Google Project Zero,
[3] G DATA Advanced Analytics, [4] University of Pennsylvania and University of Mary
[5] Graz University of Technology, [6] Cyberus Technology,
[7] Rambus, Cryptography Research Division, [8] University of Adelaide and Data61

Tor: The Second-Generation Onion Router

Roger Dingledine
The Free Haven Project
arma@freehaven.net

Nick Mathewson
The Free Haven Project
nickm@freehaven.net

Paul Syverson
Naval Research Lab
syverson@itd.nrl.navy.mil

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 better 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).**

Introductions

- **On notecards, please write down your:**
  - *Name*
  - *Pronouns*
  - *Program + Year in program*
  - *Research area*
  - *Prior experience with security (none is okay!)*
  - *What brings you to this course*
  - *Anything else you'd like me to know*

Why Security & Privacy?

- Critical lens
- Breadth and flexibility
- Problems that really matter for people
- Fun! (Lets you be a little sneaky)

This course will teach you useful skills and perspectives, regardless of your research area!

Course Structure / Expectations

- **Research readings and discussions**
  - Reading papers
  - Writing responses
  - Participating in class
- **Group-based research project**
  - Checkpoints throughout the quarter
- **Some other small assignments**

Course Structure

- Two meetings per week: W/F 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 (~2x 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!**
- A few guest lectures (TBD)

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**

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 original!** For example:
  - Paper summary, key points
  - Evaluation, opinions, response to others’ opinions
  - 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

Words of Caution

- Please don’t just use ChatGPT y’all
  - Might as well not take this class then
  - Do you want reviewers to use ChatGPT to write reviews for your papers? 😭
- Okay (and important) to critique papers, but also consider: **why was this paper accepted?**

Expectations for Reading Papers

- You will not understand everything in every paper!
  - **That is okay and expected!**
  - 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
- Strategies for reading
  - **Not like a novel!**
  - **Read some parts more closely:** Introduction, Methods (maybe), High-level design, Results (maybe), Discussion
  - Okay to read some parts less closely, depending on what you are reading for: Related Work, Methods (maybe), Implementation, Evaluation (maybe)
  - See http://ccr.sigcomm.org/online/files/p83-keshavA.pdf
    - You probably only need 1st pass for most papers (2nd pass if you are leading the discussion)

Sample Topics [in no particular order]

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

Computer Security Publication Venues

- USENIX Security
- IEEE Symposium on Security & Privacy (aka “Oakland” or S&P)

- 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 (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
- You may work individually or (preferably) in groups of 2-3
- **Follow specific format on website**

Research Project

- Groups of 2-3 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 great, publication-worthy** [parts of] projects!

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
  - Final report
  - Summary of contributions

Project presentations:
March 11, 2024
(time TBD)

Today's Discussion

Find a new person to talk to (2x):

(1) Thinking about your own current research (if any), what are some security, privacy, or safety considerations?

(and/or)

(2) What security, privacy, or safety topics are on your mind due to current events, emerging technologies, or otherwise?