CS80S - Theory and practice of secure systems

Fall 2024

Tue / Thu : 2 pm to 3:30 pm

Shravan Narayan

UT Austin

Who am I?

Assistant professor in Computer Security (https://shravanrn.com)

- Building secure systems
- Program language techniques for security
- Leveraging hardware/CPU for security

Tell me about yourselves!

- Undergrad / Masters / PhD
- Still deciding whether you're taking this course?
- Were you in my Fall 2023 course?

Today

- Course details
- How to read research papers

Course details

Website: https://shravanrn.com/teaching.html
Syllabus: https://shravanrn.com/classes/fall2024_cs380S_syllabus.pdf
Canvas: https://utexas.instructure.com/courses/1402120

Contact: shr@cs.utexas.edu

Office hours: 3:30 pm to 4:30 pm at GDC 6.430 on Tue / Thu
(Email to let me know you're coming, or if you need alternate times)

TA/Grader: Aashish Gottipati agottipati@utexas.edu

Course objectives

- Think critically about security and system designs
- Objectively read research papers
- Work on a research project that secures real applications
- Present your project/research results

Course style

Read and discuss 1 or 2 papers / class meeting

- Short writing assignments due before each class
- One student will present the paper (30 mins) + Q&A (10 mins)

Work on a large security project

- Chose by Sept 25th, 50% of the grade
- Work in progress writeup on October 26th
- Final presentations (Dec 3rd and Dec 5th) and writeup (Dec 6th)

Course difficulty

This is meant to be a challenging course

- Harder than seminar courses
- More content than prior iterations

Evaluated at a graduate course level for **everyone**

It has continuous work

- Ensure you don’t have a very large course load
- Do not take this course if you cannot regularly attend class, submit writeups

Open project counts for 50% of your grade

- Requires time
- Do not take this course if you cannot participate in a substantial project.

Grading (Explained in full in the syllabus)

Class attendance (twice a week)	10%
Paper writeups (twice a week)	20%
Paper presentations (once or twice a semester)	20%
Class project midterm writeup (once on Oct 26th)	15%
Class project final presentation (once on Dec 3rd or Dec 5th)	15%
Class project final writeup (once on Dec 6th)	20%
Bonus: class participation (throughout the semester)	5%

Attendance (10%)

Presentation + discussion based class. In-person attendance is required.

If you are sick, take the time to recover before returning to class.

4 paper skips + 2 class skips, no questions asked. What does this mean?

- You can’t show up to class: use up a class skip
- You can’t do the paper writeup (on time): use up a paper skip
- Beyond 4 paper skips or 2 class skips, follow standard UT guidelines

Last week of class is required attendance to present your project

Paper writeups starting week 2 (20%)

Summarize the paper

- Main points, 2-3 paragraphs
- Exemplary summaries may be posted on course site

Answer some questions

- Goal: think deeply about the paper
- Non-goal: testing you

Paper presentation (20%)

Lead the discussion on one (maybe two) papers

- Sign up to present a paper here (Replace "<fill in>" with your name)
- Read the paper thoroughly and skim related work
- (Optionally) talk to me prior to the class for additional resources, tips, etc.
- Prepare a 40 min presentation = 30 min content + 10 mins for discussion/Q&A

As an example: Senior PhD students will do this in the first class of next week

For everyone: Come to class prepared to discuss the paper

- Read the paper 2-3 times (small details matter), submit the writeup
- Come to class with thoughts, questions for the presenter. No discussions = no fun
- Question the problem statement, assumptions, solution, evaluation … everything!

Project: presentations + writeups (50%)

Original research / research project listed in the syllabus

- Build a new system or extend an existing one
- Reimplement the results of an existing paper
- … Others ...

PhD students: Check if you can use your (security) research for the project

Masters / Undergrad: Course project is a steppingstone to research/thesis

Project can be individual or groups up to 3

Project: presentations + writeups (50%)

Midterm writeup (15%)

- 2-page work-in-progress writeup

Final presentation (30%)

- 3rd Dec and 5th Dec
- There will be links on Canvas to sign up
- 15 minute presentation

Final writeup (15%)

- 5-page writeup

Note: Projects may require more storage than available in lab computers

Collaboration policy: collaborate!

Talk to each other

- Good ideas come from talking to smart people

Paper writeups

- Write your own, but discuss after submission and in class

Project

- Talk to others about your project
- If working in a group project, make sure to talk within the group

Prerequisites

Undergraduate security and programming languages

- Some familiarity + willingness to learn

If you're not familiar with something: ask!

- I can post external resources (e.g., book chapters)
- Ask questions in class
- Come to office hours

Not knowing something is okay!

Academic integrity and AI

Recall the Student Honor Code

> As a student of The University of Texas at Austin, I shall abide by the core values of the University and uphold academic integrity.

Students who violate University rules on academic dishonesty are subject to disciplinary penalties, including failure in the course and/or dismissal from the University.

We may use 3rd party software to detect academic integrity violations

The use of AI tools (such as ChatGPT) in this class is strictly prohibited.

Today

- Course details
- How to read research papers

How to read research papers

How to read a paper S. Keshav (2007)'s three pass approach

- 1st pass: General idea. Titles, headings, contributions, conclusions.
- 2nd pass: Read the text but ignore low-level details. Look at figures.
- 3rd pass: Read everything while mentally re-implementing the paper

Additional suggestions / tips

- Look at the authors other papers / areas of expertise
- If paper cites a "foundational" work, skim that
- Look for follow-up work that summarizes the current paper

For the next class

Next class's assigned reading (no paper writeup)

Sections 1 to 4 from
Transient-Execution Attacks: A Computer Architect Perspective
Luís Fiolhais, Leonel Sousa (2023)

Make sure to keep an eye on (and do!) the assigned readings
Readings listed in the calendar in the course syllabus
Keep an eye on this, and be prepared for discussions ☺

Module 1: Side-channel attacks & defenses

Transient-Execution Attacks: A Computer Architect Perspective

Luís Fiolhais, Leonel Sousa (2023)

Normal attacks: Learn data due to bugs in hw/sw (buffer overflows)

Side-channel attacks: Learn data by measuring indirect effects of hw/sw impls. (caches)

Architectural concepts

- Caches and cache hierarchy
- Translation lookaside buffer (TLB) and page table entries (PTE)
- Superscalar, Instruction-level parallelism (ILP)
- Out of order execution (OOO)
- Reorder buffer (ROB)
- Branch predictors & Speculative execution
- Microcode

Security – there is always news!

https://www.troyhunt.com/inside-the-3-billion-people-national-public-data-breach/

Inside the "3 Billion People" National Public Data Breach

14 AUGUST 2024

I decided to write this post because there's no concise way to explain the nuances of what's being described as one of the largest data breaches ever. Usually, it's easy to articulate a data breach; a service people provide their information to had someone snag it through an act of unauthorised access and publish a discrete corpus of information that can be attributed back to that source. But in the case of National Public Data, we're talking about a data aggregator most people had never heard of where a "threat actor" has published various *partial* sets of data with no clear way to attribute it back to the source. And they're already the subject of a class action, to add yet another variable into the mix. I've been collating information related to this incident over the last couple of months, so let me talk about what's known about the incident, what data is circulating and what remains a bit of a mystery.