CS395T - Securing real-world systems

Fall 2023

Tue / Thu : 3:30 pm to 5 pm

Shravan Narayan

UT Austin

Who am I?

New assistant professor

- PhD at UC San Diego (with Deian Stefan)

My interests

- Building secure systems
- Program language techniques for security
- Hardware-based security.

https://shravanrn.com

(Presentation format borrowed from Deian Stefan)

Tell me about yourselves!

Today

- Course details
- How to read research papers

Course details

Course website with syllabus: https://shravanrn.com/teaching.html

Canvas website will be setup for next week for assignment submissions.

Contact: shr@cs.utexas.edu

Office hours: 2:30 pm to 3:30 pm at GDC 6.430 on Tue / Thu
(Email to let me know you're coming, or if you need alternate times)

Course objectives

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

Course style

Read and discuss 1 paper / class meeting

- Short writing assignments due before each class
- Most class time will be spent discussing papers

Work on a relatively large project

- Work in progress presentation and writeup at the end of October
- Final presentations and writeup at the end of the semester

Grading (Explained in full in the syllabus)

Class attendance	10%
Paper writeups	30%
Paper presentations	10%
Class project midterm presentation and writeup	20%
Class project final presentation and writeup	30%
Bonus: class participation	5%

Attendance (10%)

Discussion based class. In-person attendance is required.

Up to 3 skips with no questions asked. What does this mean?

- You didn’t do the writing assignment (in time): use up a skip
- You can’t show up to class: use up a skip
- Beyond 3 skips, follow standard UT guidelines

Last week of class is required attendance to present your project

Note: Class on September 7th is expected to be over zoom

Paper writeups starting week 2 (30%)

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
- Exemplary/interesting answers may be posted on site

Paper presentation (10%)

Lead the discussion on one or two papers

- Choose a paper (we'll do this next class)
- Prepare discussion notes (to be posted on site), questions/comments
- Read some related work and (optionally) talk to me prior to the class

I'll lead a discussion this Thursday as an example

For everyone else: Come to class prepared to discuss paper

- Come with feedback, thoughts, questions. No discussions = no fun
- Read paper 2-3 times, small details matter
- Question the problem statement, assumptions, solution, evaluation … everything!

Project: presentations + writeups (50%)

Work on original research / try a research project listed in the syllabus

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

PhD students: Can use your research for the project (confirm with me first)

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

Project can be individual or groups up to 3.

Project: presentations + writeups (50%)

Midterm presentations (20%)

- 24 Oct 2023 and 26 Oct 2023
- 10 to 15 minute presentation
- 2 page writeup

Final presentation(30%)

- 28 Nov 2023 and 30 Nov 2023
- 15 to 20 minute presentation
- 5 page writeup

Collaboration policy: collaborate!

Talk with each other

- Good ideas come from talking to smart people

Writing assignments

- 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!

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 "seminal/foundational" work, skim that

For the next class

Next class's assigned reading (no paper writeup)

How Memory Safety Violations Enable Exploitation of Programs

Matthias Payer (2018)

Make sure to keep an eye and do the assigned readings

Readings listed in the calendar in the course syllabus

Keep an eye on this, and be prepared for discussions ☺