UNIVERSITY OF CALIFORNIA
UC RIVERSIDE

CS 250 Software Security

Spring 2026

Heng Yin
Homepage: https://www.cs.ucr.edu/~heng/
Email: heng@cs.ucr.edu

What is this course about?

Check our course homepage:

https://www.cs.ucr.edu/~heng/teaching/cs250-sp26/index.html

What problems do we want to solve?

DARPA Cyber Grand Challenge (CGC):
https://www.darpa.mil/research/programs/cyber-grand-challenge

DARPA AI Cyber Challenge (AIxCC):
https://aicyberchallenge.com/

What topics will be covered?

Vulnerability Discovery	Greybox Fuzzing Symbolic Execution Hybrid Fuzzing: Fuzzing + Symbolic Execution
Binary Reverse Engineering	Disassembly Indirect Jump/Call Resolution Data Structure and Type Recovery
Patching	Binary Rewriting Generic Patching:Vulnerability-Specific Patching
Exploit Generation	Control-flow Hijacking Data-only Attacks
Software Supply Chain Security	1-day Vulnerability Detection Binary Code Similarity Detection Binary Diffing

Lectures

First four to five weeks:

I will give lectures to provide the essential background

Project Assignments

- Project 1: Experiment with Fuzzing
  - 1.5 week
- Project 2: Experimenting with Symbolic Execution
  - 1.5 weeks
- Project 3: Implementing CFI for Binary
  - 1.5 weeks

Research Project

Research Proposal

Due by Week 5.

Term Paper

Due on June 14.

Paper Review

- Week 6 to Week 10:
  - For each lecture, read all papers and pick one paper to write review.
- Review due the day before class.
- Requirements
  - No less than 400 words.
  - No copy and paste from the original papers. **No LLMs.**
  - No bullet points.
  - Use your own natural language, show your own thinking.
- Answer these questions:
  - What problem does it solve? Why is it important?
  - What are existing solutions? Why are they not sufficient?
  - How does this paper solve the problem? Some level of details are necessary
  - What you like or dislike about this paper?
  - A list of questions you would like to discuss.

Paper Presentation

- Each student picks one or two papers to present
- 25 minutes long (Q&A excluded)
- Reusing authors' slides is fine, but may need to include additional slides for background and discussions
- Prepare several discussion questions and lead the discussion
- You are encouraged to share your slides with me in advance to get feedback

Grading Policy

	Percentage
Class Participation	10%
Project Assignments	30%
Paper Review	10%
Presentation	20%
Research Proposal	5%
Term Paper	25%