

# CS 250 Software Security

Spring 2025

Heng Yin

Homepage: <https://www.cs.ucr.edu/~heng/>

Email: [heng@cs.ucr.edu](mailto:heng@cs.ucr.edu)

# What is this course about?

Check our course homepage:

<https://www.cs.ucr.edu/~heng/teaching/cs250-sp25/index.html>

# What problems do we want to solve?

DARPA Cyber Grand Challenge (CGC):

<https://www.darpa.mil/program/cyber-grand-challenge>

DARPA AI Cyber Challenge (AIxCC):

<https://aicyberchallenge.com/>

# What skills do I need to have?

- 🔗 OS: Linux Distributions, Docker, Vagrant, WSL
- 🔗 Programming Languages: Proficient in C/C++, Python, and Java (sometimes)
- 🔗 GitHub
- 🔗 Used and modified open-source projects in the past
- 🔗 Know how to read assembly language (x86)
- 🔗 Took a computer security course (at least undergraduate level)

# What topics will be covered?

## 🔗 Vulnerability Discovery

- 🌿 Greybox Fuzzing
- 🌿 Symbolic Execution
- 🌿 Hybrid Fuzzing: Fuzzing + Symbolic Execution

## 🔗 Patching

- 🌿 Binary Rewriting
- 🌿 Indirect Jump/Call Resolution
- 🌿 Data Structure Recovery
- 🌿 Generic Patching: Shadow Stack, Stack Canary, CFI, DFI, CPI, etc.
- 🌿 Vulnerability-Specific Patching

## 🔗 Exploit Generation

- 🌿 Control-flow Hijacking
- 🌿 Data-only Attacks

## 🔗 Software Supply Chain Security

- 🌿 1-day Vulnerability Detection

Techniques: Program Analysis + AI

# Lectures



First four to five weeks:



I will give lectures to provide the essential background

# Lab Assignments

- Lab 1: Construct simple exploits from binary code
  - One week
- Lab 2: Experimenting with Fuzzing and Symbolic Execution
  - Two weeks
- Lab 3: Implementing CFI for Binary
  - Two weeks

# Research Project

 Research Proposal  
 Due by Week 5.

 Term Paper  
 Due on June 15.



# 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 ChatGPT.**
  - ✎ 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 paper 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 (Tentative)

- ✂ Class Participation: 10%
- ✂ Lab Assignments: 30%
- ✂ Paper Review: 10%
- ✂ Paper Presentation: 20%
- ✂ Research Proposal: 5%
- ✂ Term Paper: 25%