

CSE 643: Computer Security

Instructor: Dr. Yuzhe Tang, Email: ytang100@syr.edu, Office: 4-193 CST

Course Description

This course is intended for students in computer science, computer engineering, and cybersecurity. It is a 3-credit course.

The course covers attacks, vulnerabilities, and defense mechanisms in both classic and emerging application domains, including **systems software, web/blockchains, and AI systems**. A key theme of the course is understanding how the same vulnerability can reappear across different applications. For example, race conditions occur in systems software and can also manifest in smart contracts to enable reentrancy attacks.

For security in systems software and web applications, the course uses Dr. Kevin Du's SEED Labs. For blockchain security, the course uses Dr. Yuzhe Tang's BADD Labs.

The course emphasizes the "security for AI," focusing on how security issues arise in AI system stack, including agent, RAG, prompt engineering, etc.

Learning Objectives

Students will be able to 1) understand common cyber-security threats in systems programs, web applications, blockchains, and AI systems, 2) defense designs to protect these applications against the threats.

Texts

Lecture slides are required readings.

Optional materials

- Computer & Internet Security, Wenliang Du (3rd or 2nd edition)
 - Desk copy: Bird Library, Carnegie Library
 - Resources: <https://www.handsonsecurity.net/resources.html>
- Hacking: The Art of Exploitation, 2nd Edition: Jon Erickson
- Mastering Ethereum: Smart contract and decentralized applications, [\[online book\]](#)

Grading

- Labs / Exercises: 50%
- Course Project: 50%
 - Option 1: Technical review & presentation
 - Option 2: Hands-on project & demo

Policies

- Late submission: 10% off within one day, 40% off within two days, 50% off within three days, 70% off within one week.
- All labs have to be finished individually; no collaboration will be allowed.
- No copy-and-paste is allowed in any circumstances.
- Any questions about grading should be directed to Dr. Tang.