USC Viterbi
School of Engineering

CSCI 499: Software and Hardware Security

Units: 4.0
Fall 2025 — Thursdays — 4:00-7:20PM

Location: THH 217

Instructor: Weihang Wang
Office: TBD
Office Hours: TBD
Contact Info: weihangw@usc.edu

Catalogue Description

Principles and practices of software/hardware security, including core security concepts, binary-level software analysis, assembly programming, reverse engineering, side channels, binary exploitation, and cryptographic vulnerabilities.

Course Description

Software and hardware security are fundamental to safeguarding computer systems. Software vulnerabilities, such as bugs or design flaws, can be exploited to gain unauthorized access, steal data, or execute malicious actions, while hardware vulnerabilities, including flaws in physical devices, can lead to system manipulation or compromise.

This course provides an in-depth exploration of the principles and practices of software and hardware security, equipping students with the skills to analyze, protect, and understand the vulnerabilities of modern systems. As cyber threats continue to evolve, understanding how software operates at the binary level is crucial for developing robust defenses. Students will learn core security concepts, assembly programming, and reverse engineering techniques using tools such as Ghidra. They will also engage with real-world challenges, including binary exploitation, cryptographic vulnerabilities, and security in autonomous and embedded systems. By the end of the course, students will develop critical thinking and practical skills to detect and mitigate threats, making them well-prepared for careers in cybersecurity, software development, or research. This course is ideal for students seeking a deeper understanding of system security or aiming to enhance their defensive and analytical capabilities.

Learning Objectives

The course aims to equip students with both theoretical knowledge and practical expertise in software and hardware, preparing them to tackle the challenges of securing modern systems. In particular, the focus of this course is on equipping students with the knowledge and hands-on experience needed to understand, analyze, and defend systems against security threats, with a strong emphasis on reverse engineering and vulnerability exploitation.

Upon completion of the course, students will be able to:

1. Understand core security principles:
Students will gain a foundational understanding of key computer security concepts, including encryption, authentication, access control, and secure coding practices. They will explore how vulnerabilities arise in software and hardware, the different types of attacks (e.g., buffer overflows, side-channel attacks), and the fundamental principles that guide effective defense strategies. This knowledge forms the basis for evaluating system security and designing secure systems.

2. Develop reverse engineering skills:
Through hands-on experience with Ghidra, students will acquire the skills to reverse engineer software and hardware. This includes the ability to analyze machine code, identify control flow, and understand the structure of binaries and firmware. By learning to dissect software at the binary level, students will gain insights into how malicious code operates and how vulnerabilities can be uncovered.

3. Identify and exploit vulnerabilities:
Students will be able to identify common security weaknesses in both software and hardware, such as memory corruption bugs, race conditions, and insecure cryptographic practices. They will also develop the ability to exploit these vulnerabilities in a controlled environment, such as through buffer overflows or privilege escalation techniques. This hands-on experience enables students to understand attack strategies, which is essential for building better defenses.

4. Secure software and hardware systems:
Using the skills developed in reverse engineering, students will apply practical defense techniques to secure software applications and embedded systems. They will examine how to patch vulnerabilities,

implement secure coding practices, and harden systems against attacks. This objective emphasizes proactive security measures, such as code analysis and secure design principles, to minimize the risk of exploitation.

5. Prepare for real-world cybersecurity challenges:
Students will be encouraged to think critically and approach problems like attackers and defenders, developing a deep understanding of how security is tested in real-world scenarios. By working on projects and case studies, students will hone their ability to adapt to new threats, build resilience into systems, and respond to evolving cybersecurity challenges. This objective prepares students for careers in cybersecurity, software engineering, or research by giving them practical skills.

Recommended Preparation

The course assumes that students have general proficiency in system programming with C/C++ and familiarity with basic concepts in software testing and compilers. A background in C/C++ programming (at the level of CSCI 104) and computer security (at the level of CSCI 430) is recommended.

Course Notes

Lecture notes will be made available online after each class.

Technological Proficiency and Hardware/Software Required

Homework assignments will require a Linux environment. Students should be prepared to set up a virtual machine if they do not use Linux as their native operating system. Using VirtualBox or WSL is recommended. Students in this course should be familiar with the usage of the ACM Digital Library and Google Search.

Required Readings and Supplementary Materials

Textbooks are not mandatory for this course. The instructor will provide lecture notes. Additionally, the following books are suggested as optional supplementary reading materials:

- Foundations of Software Testing: Fundamental Algorithms and Techniques, by Aditya P. Mathur
- Exploiting Software: How to Break Code, by Greg Hoglund and Gary McGraw
- The Ghidra Book: The Definitive Guide, by Chris Eagle and Kara Nance
- Practical Reverse Engineering by Bruce Dang, Alexandre Gazet, and Elias Bachaalany

Description of Assignments and How They Will Be Assessed

The course will consist of two homework assignments, one project, two quizzes, and a final exam.

Homework assignments:
There will be two homework assignments. Each homework assignment, which accounts for 20% of the grade, will consist of conducting security analysis using reverse-engineering techniques via Ghidra. All homework assignments must be submitted electronically.

In class quizzes and final exam:
The course will include two in-class quizzes, both of which will be structured as multiple-choice questions. These quizzes are designed to assess students' understanding of key concepts in computer security and reverse engineering. After each quiz, the answers and detailed explanations will be reviewed in class to ensure that students fully grasp the material. This review process will not only reinforce learning but also provide valuable insights into common pitfalls and key takeaways. Additionally, the content covered in the quizzes will serve as a foundation for the final exam, allowing students to solidify their knowledge of critical concepts that will be essential for their success in the course. The quizzes thus provide an opportunity for continuous learning and reflection.

Semester project:
The semester project provides students with hands-on experience in reverse engineering and network traffic analysis to identify and mitigate malicious behavior. Students will reverse-engineer a binary executable to understand its functionality, focusing on how it handles network communication and generates outbound traffic. They will analyze captured network payloads to uncover patterns, potential vulnerabilities, and the intent behind the data exfiltration. By identifying system calls and behaviors that can be monitored for detection, students will learn how to design strategies to recognize similar threats in the future. The project emphasizes practical skills in malware analysis, network security, and detection techniques, preparing students to address real-world cybersecurity challenges.

Participation
This is a discussion-based course, thus regular attendance is expected. Lack of attendance will affect the class participation score. Missed classes with a valid reason are allowed. Class participation, constituting 10% of the grade, will be scored based on engagement in course discussions.

Grading Breakdown

Assessment Tool (assignments)	**% of Grade**
Homework	20%
Semester project	40%
Participation	10%
Quiz and final exam	30%
TOTAL	100%

Grading Scale
Course final grades will be determined using the following scale:

Letter grade	Corresponding numerical point range
A	95-100
A-	90-94
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66
D-	60-62
F	59 and below

Assignment Submission Policy
All homework assignments (including code) and project reports will be submitted electronically using the USC Brightspace system. Assignments are due at 11:59pm on the due date.

Course-Specific Policies
Late submissions will not be accepted unless the student has a documented emergency that prevented on-time completion and submission.

Attendance
Students are expected to attend all classes in person. In rare circumstances, the instructor may approve attending via Zoom; prior approval is required. Virtual attendees must remain actively engaged, keep their

camera on, and contribute to discussions. If a session is missed, students can review the online materials provided.

Academic Integrity for this Class

Unless otherwise noted, this course will follow the expectations for academic integrity as stated in the USC Student Handbook. The general USC guidelines on Academic Integrity and Course Content Distribution are provided later in this syllabus.

For this class, students are expected to submit work that demonstrates their individual mastery of the course concepts. Unless specifically designated as a 'group project,' all assignments are expected to be completed individually. Plagiarism includes the submission of code written by, or otherwise obtained from someone else.

If found responsible for an academic violation, students may be assigned university outcomes, such as suspension or expulsion from the university, and grade penalties, such as an "F" grade on the assignment, exam, and/or in the course.

Please ask the instructor [and/or TA(s)] if you are unsure about what constitutes unauthorized assistance on an exam or assignment, or what information requires citation and/or attribution.

Class Recordings and Course Content Distribution: You may not record this class without the express permission of the instructor and all other students in the class. Distribution of any notes, recordings, exams, or other materials from a university class or lectures — other than for individual or class group study — is prohibited without the express permission of the instructor; violations will be considered an intentional act to facilitate or enable academic dishonesty and reported to the university.

Use of Generative AI in this Course

Generative AI is not permitted: This course aims to develop creative, analytical, and critical thinking skills. Therefore, all assignments should be prepared by the student working individually or in groups as described on each assignment. Students may not have another person or entity complete any portion of the assignment. Developing strong competencies in these areas will prepare you for a competitive workplace. Therefore, using AI-generated text, code, or other content is prohibited in this course, will be identified as plagiarism, and will be reported to the Office of Academic Integrity.

Course Evaluations

The course will include both mid-semester and end-of-semester evaluations. The mid-semester evaluation will take place around Week 7, offering students an opportunity to provide constructive, anonymous feedback on the course. This feedback will allow the instructor to address any concerns and make necessary adjustments to improve the course content, teaching methods, and overall student experience. The end-of-semester evaluations will be conducted during the last few class meetings, with the instructor stepping out while the teaching assistant supervises the process. During this time, students will complete their evaluations, providing comprehensive feedback on the course's effectiveness, which will be used to inform future course improvements.

Course Schedule

	Topics/Daily Activities	Readings/ Preparation	Deliverables
Week 1	**Introduction and Logistics** Overview of the course, expectations, and introduction to security concepts.	- Syllabus - Learn RE: but where to start? (https://yurichev.org/RE_start/)	
Week 2	**Security Concepts** Introduction to core security principles, followed by details of compilers, disassemblers and decompilers.	- Practical Reverse Engineering (Chapter 2).	
Week 3	**Software Security** Focus on software vulnerabilities and techniques for securing software, alongside learning x64 assembly language for understanding low-level operations.	- Introduction to x64 Assembly by Intel. - Intel x86/64 Instruction Set Manual	
Week 4	**Hardware Security** Exploration of hardware security issues, including hardware-based attacks and defenses.	- Rowhammer: Flipping Bits in Memory by Project Zero	Homework 1 assigned
Week 5	**Autonomous Vehicle Security** Security challenges and risks in autonomous vehicles, including potential vulnerabilities and attack vectors.	- The Autonomous Driving Cookbook by Microsoft (https://github.com/microsoft/AutonomousDrivingCookbook)	
Week 6	**Autonomous Vehicle Security (cont.)** Deeper dives into real-world applications and defenses of autonomous vehicle security.	- CARLA Simulator (https://carla.org/)	
Week 7	**Side Channels and Attacks** Side-channel attacks, which exploit indirect information from systems to break security mechanisms	- Side-channel attacks: A short tour by Frank Piessens and Paul C. van Oorschot	Homework 1 due Homework 2 assigned
Week 8	**Side Channels and Attacks (cont.)** Further exploration of side-channel attacks, focusing on detection and mitigation strategies.	- Meltdown and Spectre: https://meltdownattack.com/	
Week 9	**Operating Systems Security** Understanding OS-level security concerns, including process management, access control, and defenses.	- Operating System Security by Trent Jaeger	
Week 10	**Operating Systems Security (cont.)** Continuation of OS security topics, with a focus on practical defense mechanisms.	- Footprinting: What Is It, Who Should Do It, and Why? by James McGreevy	Homework 2 due Final Project assigned
Week 11	**Operating Systems Security (cont.)** Further discussion on OS security, including advanced attack vectors and mitigation techniques.		
Week 12	**Cyber Physical Systems Security** Introduction to the security of cyber-physical systems, covering potential vulnerabilities and attack methods.	- OWASP Top 10 Drone Security Risks (https://owasp.org/www-project-top-10-drone-security-risks/)	
Week 13	**Cyber Physical Systems Security (cont.)**: Exploration of cyber-physical systems security, with additional examples and real-world case studies.	- Soaring Security: How Drones Are Redefining Penetration Testing by pentestmag.com	
Week 14	**Class Recap/Review** A review of the key topics covered throughout the course to reinforce critical security concepts.		Final Project due
Week 15	**Project Review** A review of the final project submissions and solutions.		
FINAL	**In-class Final Exam.** Comprehensive assessment covering all course material.		Refer to the final exam schedule in the USC *Schedule of Classes* at classes.usc.edu.

Academic Integrity

The University of Southern California is foremost a learning community committed to fostering successful scholars and researchers dedicated to the pursuit of knowledge and the transmission of ideas. Academic misconduct — which includes any act of dishonesty in the production or submission of academic work (either in draft or final form) — is in contrast to the university's mission to educate students through a broad array of academic, professional, and extracurricular programs.

This course will follow the expectations for academic integrity as stated in the USC Student Handbook. All students are expected to submit assignments that are their own original work and prepared specifically for this course and section in this academic term. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s). Students suspected of engaging in academic misconduct will be reported to the Office of Academic Integrity.

Other violations of academic misconduct include, but are not limited to, cheating, plagiarism, fabrication (e.g., falsifying data), knowingly assisting others in acts of academic dishonesty, and any act that gains or is intended to gain an unfair academic advantage.

Academic dishonesty has a far-reaching impact and is considered a serious offense against the university. Violations will result in a grade penalty, such as a failing grade on the assignment or in the course, and disciplinary action from the university itself, such as suspension or even expulsion.

For more information about academic integrity see the student handbook or the Office of Academic Integrity's website, and university policies on Research and Scholarship Misconduct.

Please ask your instructor if you are unsure what constitutes unauthorized assistance on an exam or assignment or what information requires citation and/or attribution.

Course Content Distribution and Synchronous Session Recordings Policies

USC has policies that prohibit recording and distribution of any synchronous and asynchronous course content outside of the learning environment.

Recording a university class without the express permission of the instructor and announcement to the class, or unless conducted pursuant to an Office of Student Accessibility Services (OSAS) accommodation. Recording can inhibit free discussion in the future, and thus infringe on the academic freedom of other students as well as the instructor. (Living our Unifying Values: The USC Student Handbook, page 13).

Distribution or use of notes, recordings, exams, or other intellectual property, based on university classes or lectures without the express permission of the instructor for purposes other than individual or group study. This includes but is not limited to providing materials for distribution by services publishing course materials. This restriction on unauthorized use also applies to all information, which had been distributed to students or in any way had been displayed for use in relation to the class, whether obtained in class, via email, on the internet, or via any other media. Distributing course material without the instructor's permission will be presumed to be an intentional act to facilitate or enable academic dishonestly and is strictly prohibited. (Living our Unifying Values: The USC Student Handbook, page 13).

Statement on University Academic and Support Systems

Students and Disability Accommodations:
USC welcomes students with disabilities into all of the University's educational programs. The Office of Student Accessibility Services (OSAS) is responsible for the determination of appropriate accommodations for students who encounter disability-related barriers. Once a student has completed the OSAS process (registration, initial appointment, and submitted documentation) and accommodations are determined to be reasonable and appropriate, a Letter of Accommodation (LOA) will be available to generate for each course. The LOA must be given to each course instructor by the student and followed up with a discussion. This should be done as early in the semester as possible as accommodations are not retroactive. More information can be found at osas.usc.edu. You may contact OSAS at (213) 740-0776 or via email at osasfrontdesk@usc.edu.

Student Financial Aid and Satisfactory Academic Progress:
To be eligible for certain kinds of financial aid, students are required to maintain Satisfactory Academic Progress (SAP) toward their degree objectives. Visit the Financial Aid Office webpage for undergraduate- and graduate-level SAP eligibility requirements and the appeals process.

Support Systems:
Counseling and Mental Health - (213) 740-9355 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

988 Suicide and Crisis Lifeline - 988 for both calls and text messages – 24/7 on call
The 988 Suicide and Crisis Lifeline (formerly known as the National Suicide Prevention Lifeline) provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week, across the United States. The Lifeline consists of a national network of over 200 local crisis centers, combining custom local care and resources with national standards and best practices. The new, shorter phone number makes it easier for people to remember and access mental health crisis services (though the previous 1 (800) 273-8255 number will continue to function indefinitely) and represents a continued commitment to those in crisis.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL) – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender- and power-based harm (including sexual assault, intimate partner violence, and stalking).

Office for Equity, Equal Opportunity, and Title IX (EEO-TIX) - (213) 740-5086
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-2500
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office for Equity, Equal Opportunity, and Title for appropriate investigation, supportive measures, and response.

The Office of Student Accessibility Services (OSAS) - (213) 740-0776
OSAS ensures equal access for students with disabilities through providing academic accommodations and auxiliary aids in accordance with federal laws and university policy.

USC Campus Support and Intervention - (213) 740-0411
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity, Equity and Inclusion - (213) 740-2101
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-1200 – 24/7 on call
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.

Occupational Therapy Faculty Practice - (323) 442-2850 or otfp@med.usc.edu
Confidential Lifestyle Redesign services for USC students to support health-promoting habits and routines that enhance quality of life and academic performance.