USC Viterbi
School of Engineering

CSCI 599: Software Engineering for Security

Units: 4.0

Fall 2024 – Fridays – 1:00-4:20PM

Location: TBD

Instructor: Weihang Wang
Office: SAL 342
Office Hours: TBD
Contact Info: weihangw@usc.edu

Catalogue Description
Application of software testing and program analysis techniques for software security.

Course Description
Software serves as a fundamental cornerstone within cyber systems, making it a prime target for cyber attackers. These malicious actors invest substantial efforts in understanding computing systems, especially software, in order to exploit vulnerabilities and fulfill their malicious objectives. Simultaneously, from a defender's standpoint, software occupies a pivotal position in terms of security. It serves as the interface with underlying hardware and users, including potential attackers. Essentially, software acts as the gateway for all crucial security components, presenting an ideal opportunity to implement robust security measures.

Learning Objectives
The objective of this course is to acquire knowledge on developing secure computing systems through the application of software engineering techniques. The focus lies in gaining insights into attackers and their methodologies for system exploitation. By delving deeply into the understanding of attacker strategies, the course also aims to equip students with the skills to construct secure software systems.

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

1. **Develop a Deep Understanding of Attackers**
- Gain insights into different attacker types, motivations, objectives, and explore various threat models.
- Analyze how attackers perceive programs, identify potential targets, and assess their capabilities and potential escalation.

2. **Develop Automated Program Analysis**
- Learn the utilization of program analysis for automatic vulnerability discovery.
- Identify challenges, limitations, and ethical considerations associated with discovering vulnerabilities. Practical application of program analysis techniques will be emphasized through assignments.

3. **Construct Automated Defenses**
- Acquire skills in using program analysis to construct automated defense systems.
- Understand defense mechanisms, along with their challenges and limitations, within the context of automated systems.

Throughout the course, students will not only gain theoretical knowledge but will also engage in practical exercises and assignments to apply the concepts learned. The overarching goal is to enable students to implement secure software practices by understanding the dynamics of both attackers and defenders in the domain of software security.

Recommended Preparation
The course assumes that students have general proficiency in system programming and familiarity with basic concepts in software testing and compilers. While there are no prerequisite courses, a background in software engineering or equivalent (at the level of CSCI 310) and computer security or equivalent (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 and WSL version 2 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

Description and Assessment of Assignments

The course will consist of three homework assignments, one research paper presentation, and one semester project.

Homework assignments:

There will be three homework assignments. Each homework assignment, which accounts for 10% of the grade, will consist of a mix of short practical programming problems and theoretical questions. All homework assignments must be submitted electronically.

Research paper presentation:

The research paper presentation assignment asks each student to select a paper from a provided list of recently published papers suggested by the instructor. The goal is to deepen their understanding of the latest advancements in the field and to teach others on the selected topic. Each student is expected to identify the main problem addressed by the paper, review previous work that has been done, articulate how the chosen paper improves upon or extends existing work, and propose potential generalizations or extensions. The assessment of the research paper presentation will be based on the clarity of the presentation and the quality of the slides.

Semester project:

Students will work in small groups to carry out a class project, and the topic will be centered around web security. The tentative topic is WebAssembly-based attacks and defenses. WebAssembly is a new type of client-side web programming languages that aims to support high-performance computations on the web. Given that WebAssembly cannot access web APIs directly and can only do so via JavaScript calls, students are expected to be proficient in JavaScript programming in addition to getting familiar with WebAssembly. Below are some references for WebAssembly development and usage.

Regarding resource for WebAssembly usage, here are some links to get familiar with the WebAssembly design and usage:

https://medium.com/javascript-scene/what-is-webassembly-the-dawn-of-a-new-era- 61256ec5a8f6
https://dev.to/captainsafia/why-the-heck-is-everyone-talking-about-webassembly-455a
https://www.freecodecamp.org/news/get-started-with-webassembly-using-only-14-lines-of-javascript-b37b6aaca1e4/
https://wasmbyexample.dev/
https://developer.mozilla.org/en-US/docs/WebAssembly/C_to_wasm
https://github.com/mdn/webassembly-examples

For code development, students can use Visual Studio Code with the WebAssembly extension enabled.

Class 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.

Assignment Submission Policy

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

Use of Generative AI in this Course

Generative AI is not permitted: Since creating, analytical, and critical thinking skills are part of the learning outcomes of this course, 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 tools is prohibited in this course, will be identified as plagiarism, and will be reported to the Office of Academic Integrity.

Grading Breakdown

1. Homework: 30% (3 assignments, each 10%)
2. Semester project: 50%
3. Participation: 10%
4. Research paper presentation: 10%

Tentative Schedule

	Topics/Daily Activities	Assignment
Week 1	Introduction Program Representation	
Week 2	Dynamic Analysis	
Week 3	Intel Pin and Debugging	HW 1 out
Week 4	Project Proposal	Project proposal due
Week 5	Web Security	HW 1 deadline
Week 6	Reverse Engineering	HW 2 out
Week 7	Research Paper Presentation	
Week 8	Research Paper Presentation	HW 2 deadline
Week 9	Static Analysis	Project mid-semester report due
Week 10	Execution Perturbation	HW 3 out
Week 11	Forced Execution	
Week 12	Code Emulation	HW 3 deadline
Week 13	Symbolic Analysis	
Week 14	Fuzzing	
Week 15	Project Demo	
FINAL	Project Final Report	Due on the university-scheduled date of the final exam.

Statement on Academic Conduct and Support Systems

Academic Integrity:
The University of Southern California is a learning community committed to developing successful scholars and researchers dedicated to the pursuit of knowledge and the dissemination of ideas. Academic misconduct, which includes any act of dishonesty in the production or submission of academic work, comprises the integrity of the person who commits the act and can impugn the perceived integrity of the entire university community. It stands in opposition to the university's mission to research, educate, and contribute productively to our community and the world.

All students are expected to submit assignments that represent their own original work, and that have been prepared specifically for the course or section for which they have been submitted. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s).

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

The impact of academic dishonesty is far-reaching and is considered a serious offense against the university. All incidences of academic misconduct will be reported to the Office of Academic Integrity and could result in outcomes such as failure on the assignment, failure in the course, suspension, or even expulsion from the university.

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 relationship to the class, whether obtained in class, via email, on the internet, or via any other media. (Living our Unifying Values: The USC Student Handbook, page 13).

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.

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 is comprised 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) 740-5086 or (213) 821-8298
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.