CSE 227, Computer Security, Winter 2025

About the Course

Course Description

This graduate-level course focuses on computer security: the study of computer systems in the presence of an adversary. The course is a *breadth* course designed to give students exposure to many aspects of computer security, with topics including systems security, web security, edge security, and privacy. The course will introduce students to modern research challenges in the area and the standards for how we design safer and more secure computer systems. Students will primarily read, synthesize, present, and discuss research papers. The course will culminate in a presentation of a quarter-long research project that students will conduct in small groups.

Prerequisites

Some cybersecurity knowledge is helpful, but not required. This is a research focused course, so students who are excited to explore novel topics are encouraged to enroll.

Learning Outcomes

Upon completion of the course, students should have a solid understanding of many different types of computer security challenges, how security problems get addressed in the real world, and the tensions, challenges, and opportunities involved in doing research in this field. Students should also feel comfortable reading and engaging with current research in this area and be well equipped to conduct their own independent research in cybersecurity related areas.

Course Logistics

Instructors

Deepak Kumar, Assistant Professor in CSE
Email: kumarde@ucsd.edu
Office Hours: Tuesday 2:00–3:00 PM, or by appointment, CSE 3248.

Tianyi Shan
Email: tshan@ucsd.edu
Office Hours: By appointment

Course Resources

Course website: https://kumarde.com/cse227-w24/
Canvas: https://canvas.ucsd.edu/courses/61827

Time and Location

T/Th, 12:30 – 1:50pm, Ridge Walk Academic Complex 0121

Coursework and Grades

Assignments/Coursework

There are three primary grade-assigning mechanisms in this course:

Attendance (5%)

Attendance is mandatory in class and constitutes 5% of your grade. *You can miss up to 2 classes without penalty and without needing to justify your absence to me*. If you have additional conflicts, please contact me directly.

Participation (20%)

Most class sessions will be structured as a discussion-forward lecture run by Deepak. The primary mechanism for discussion is through *cold calls*, which are random calls to students. These questions are a mix of testing comprehension of the reading material, as well as getting students talking and discussing the topics in each paper. You get 3 "passes" over the quarter where you can skip the question if you have not read the paper. **If you have not read the paper in advance, you must disclose this when called on**. Violations of this policy amount to an Academic Integrity violation.

Term Project (75%)

Students will work on an independent research project over the term in groups of 3-4, which will culminate in a project presentation and small (~5 page) writeup. A separate specification for the project will be provided outside of this syllabus. The grade is divided into several subparts:

- **Protect Intention Form (10%)** – This form will commit your group members and the general project direction you are going in.
- **Midpoint Check-In Document & Meeting (15%)** – This 2-page document describes your current status on the project and will serve as the basis for our meeting where we discuss more about the project in detail
- **Final Presentation (25%)** – This 15-minute presentation will be given in the final week of the quarter
- **Final Writeup (25%)** – This 5-page document describes the work completed over the quarter and the project.

Course Policies

Academic Integrity

In this course we expect students to adhere to the UC San Diego Integrity of Scholarship Policy. This means that you will complete your work honestly, with integrity, and support and environment of integrity within the class for which you are tutoring. Some examples of specific ways this policy applies to Sociotechnical Cybersecurity include:

- Lying about doing the reading when you have not done the reading
- Not working collaboratively with your teammates on your term projects

Please sign the academic integrity agreement at the beginning of this term: https://academicintegrity.ucsd.edu/forms/form-integrity-agreement-cse.html

Collaboration Policy

Students may collaborate on many aspects of the course – in discussion, in slide preparation, and especially in group project settings.

AI / LLM Policy

Students may use modern LLMs, like OpenAI's GPT-suite, Google's Gemini suite, Anthropic's Claude, etc. to help with understanding the paper, but I warn you, reading summaries of these papers via these tools alone **will not** help you in discussion. The intention of this class is to have you think critically about the work happening in this space beyond a surface level. Cold-call questions will be constructed to promote deeper thinking about the paper.

Regrade Policy

If you feel a grade was inappropriately assigned or you wish to discuss, please come to office hours or contact me directly via Piazza.

Late or Missed Assignments/Missed Exam Policy

Attendance:

- You may miss up to 2 classes without telling me in advance. If you have additional conflicts please contact me; missing classes will result in a reduction of your grade.

Cold Calls:

- You may skip being cold-called up to *3 times* over the quarter when you are called on. Additional skips will result in a reduction of your grade.

Otherwise, deadlines are firm, and late work will reduce your grade **10%** for every 24-hours beyond the deadline period.

If you have a pressing emergency, like a personal conflict, illness, or other circumstance, please reach out to me and we can discuss.

Late Add Policy

The CSE department (https://cse.ucsd.edu/undergraduate/courses/enrolling-cse-courses) does not allow students to add courses past week 2. If a student is not enrolled in enough units by the beginning of week 1, the student should contact their department advisors via the VAC.
No late adds - no exceptions. EASy requests for Late Adds in the CSE Department will be denied, so please plan accordingly.

Please note, all students are expected to attend class for the first two weeks and complete assignments if they are on the waitlist for a course. Attending class and completing course assignments does not guarantee enrollment. If students choose to miss class or not turn in assignments while on the waitlist, the student will receive a "0" on all missed assignments, if they secure a seat in the course off the waitlist.

Incomplete

Sometimes, circumstances beyond a student's control prevent them from completing a class even once they have completed the majority of the coursework at a passing level. UCSD has a process in place for you to request an Incomplete (I) if this happens to you. Here is the campus policy about the Incomplete grade:
https://senate.ucsd.edu/Operating-Procedures/Senate-Manual/Regulations/500 and some information about it:
https://students.ucsd.edu/academics/exams-grades-transcripts/grades/request-remove-incomplete.html

Technology Policy

Students may use computers in class, but it should not get in the way of discussion. If you are obviously doing other activities in class on your computer, this may result in your attendance credit being taken away for that session.

Outside Tutoring

Individuals are not permitted to approach students to offer services of any kind in exchange for pay, including tutoring services. This is considered solicitation for business and is strictly prohibited by University policy.

Class material and intellectual property

Our lectures and course materials, including videos, assignments, and similar materials, are protected by U.S. copyright law and by University policy. We are the exclusive owner of the copyright in those materials we create. We acknowledge the cumulative contributions to this

course material of previous course instructors, TAs, and tutors, as well as contributions to the class structure from colleagues in CSE and at UCSD.

You may take notes and make copies of course materials for your own use. You may also share those materials with another student who is enrolled in or auditing this course. You may not reproduce, distribute or display (post/upload) lecture notes or recordings or course materials in any other way — whether or not a fee is charged — without our express prior written consent. You also may not allow others to do so. If you do so, you may be subject to student conduct proceedings under the UC San Diego Student Code of Conduct.

Similarly, you own the copyright in your original work. If I am interested in posting your answers or papers on the course web site, I will ask for your written permission.

Satisfactory Academic Progress

Satisfactory Academic Progress (SAP) refers to the academic standards students must maintain to remain eligible for federal, state, and institutional financial aid. If you are receiving financial aid, please ensure you review the SAP requirements and the appeals process. More details at this campus website: https://fas.ucsd.edu/forms-and-resources/sap/index.html .

Resources for Students

Getting Help

Students can ask questions about the course on Piazza: https://piazza.com/demo_login?nid=m5e3ck8k5ii3lq&auth=c43bcbc and reach out to me at any time if you have additional questions.

Furthermore, The IDEA Engineering Student Center, located just off the lobby of Jacobs Hall, is a hub for student engagement, academic enrichment, personal/professional development, leadership, community involvement, and a respectful learning environment for all. The Center offers a variety of programs, listed in the IDEA Center Facebook page at http://www.facebook.com/ucsdidea/ (you are welcome to Like this page!) and the Center web site at http://idea.ucsd.edu/. The IDEA Center programs support both undergraduate students and graduate students.

Diversity and Inclusion

We are committed to fostering a learning environment for this course that supports a diversity of thoughts, perspectives and experiences, and respects your identities (including race, ethnicity, heritage, gender, sex, class, sexuality, religion, ability, age, educational background, etc.). Our goal is to create a diverse and inclusive learning environment where all students feel comfortable and can thrive.

Our instructional staff will make a concerted effort to be welcoming and inclusive to the wide diversity of students in this course. If there is a way we can make you feel more included please let one of the course staff know, either in person, via email/discussion board, or even in a note under the door. Our learning about diverse perspectives and identities is an ongoing process, and we welcome your perspectives and input.

We also expect that you, as a student in this course, will honor and respect your classmates, abiding by the UCSD Principles of Community (https://ucsd.edu/about/principles.html). Please understand that others' backgrounds, perspectives and experiences may be different than your own, and help us to build an environment where everyone is respected and feels comfortable.
If you experience any sort of harassment or discrimination, please contact the instructor as soon as possible. If you prefer to speak with someone outside of the course, please contact the Office of Prevention of Harassment and Discrimination: https://ophd.ucsd.edu/.

Students with Disabilities

We aim to create an environment in which all students can succeed in this course. If you have a disability, please contact the Office for Students with Disability (OSD), which is located in University Center 202 behind Center Hall, to discuss appropriate accommodations right away. We will work to provide you with the accommodations you need, but you must first provide a current Authorization for Accommodation (AFA) letter issued by the OSD. You are required to present their AFA letters to Faculty (please make arrangements to contact me privately) and to the OSD Liaison in the department in advance so that accommodations may be arranged.

Basic Needs/Food Insecurities

If you are experiencing any basic needs insecurities (food, housing, financial resources), there are resources available on campus to help, including The Hub and the Triton Food Pantry. Please visit http://thehub.ucsd.edu/ for more information.

Student Conduct Policy

UC San Diego strives to maintain a climate of fairness, cooperation, and professionalism. It is expected that you practice basic principles, including, but not limited to, mutual respect, civility, and decency, towards maintaining an atmosphere free of abusive or demeaning treatment. Non-academic student misconduct will be reported to the Center for Student Accountability, Growth, and Education for violating UC San Diego's Principles of Community.