Course Number: EE P 595

Title: Computer Systems Security

Quarter and Year: Autumn 2025

Credits: 4

Instructor: Dinuka Sahabandu (sdinuka@uw.edu)
Instructor Office Hours: ***Saturdays (10 AM - Noon)*** **zoom**:
https://washington.zoom.us/j/92910385733

TA: Ben Davis (bldbld@uw.edu)
TA Office Hours: Tuesdays 7-9 PM **zoom**: https://washington.zoom.us/j/4254457552

Zoom Link for Class: https://washington.zoom.us/j/97942143354 [Meeting ID: 979 4214 3354]
The primary mode of instruction is in person. Use the Zoom link only when work, emergencies, or other obligations make in-person attendance impossible.

Join our Discord: https://discord.gg/gtc2nXv8

Course Goals:

This course aims to provide students with a comprehensive understanding of the principles and practices involved in securing modern computer systems. It covers a broad spectrum of system security domains, including network security, web application security, software vulnerability mitigation, and hardware attack defenses. Along with foundational trust frameworks such as Public Key Infrastructure (PKI), mutual authentication schemes, session key distribution methods, the Web of Trust (WoT), and secure communication protocols, key mechanisms covered include buffer overflow protection, access control, sandboxing, firewall configuration, and authentication protocols. Students will examine real-world attack scenarios such as Cross-Site Scripting (XSS), session hijacking, and hardware-level exploits (e.g., Spectre, Meltdown). Emphasis is placed on hands-on learning through lab-based exercises that mirror real-world environments, preparing students to critically evaluate and strengthen the security posture of computing systems in both enterprise and cloud-scale deployments.

Learning Objectives:

At the end of this course, students will be able to:

1. Explain the foundational concepts of system security, including threat models, vulnerabilities, and attack surfaces.

2. Analyze and implement secure communication protocols using PKI, session key negotiation, and mutual authentication.
3. Evaluate access control and privilege separation mechanisms in operating systems (OS).
4. Identify and mitigate software-level vulnerabilities such as buffer overflows, race conditions, and format string exploits.
5. Assess and defend against web application attacks, including Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and SQL injection.
6. Conduct network-based attacks (e.g., TCP spoofing, SYN flooding, session hijacking) in a lab environment and understand countermeasures like firewalls and Virtual Private Networks (VPNs).
7. Investigate hardware-based security issues, such as the Meltdown and Spectre attacks, and explain their impact on modern processors.
8. Perform end-to-end security analysis and articulate the design trade-offs in real-world system defenses.

Reference Textbooks:

1. Kaufman, R. Perlman, M. Speciner, Network Security: Private Communication in a Public World, 3rd Edition, Addison-Wesley, 2022.
2. Du, Computer & Internet Security: A Hands-on Approach, 3rd Edition, Self-Published, 2022.
3. Stallings, L. Brown, Computer Security: Principles and Practice, 5th Edition, Pearson, 2024.

Prerequisites:

Familiarity with programming and foundational knowledge of computer systems. No prior experience in systems or network security is required.

Topics:

1. Week 1: Network Basics and Public Key Infrastructure (PKI)
2. Week 2: Mutual Authentication Schemes, Session Key Distribution, Web of Trust (WoT)

3. Week 3: Sniffing, Spoofing, and TCP Attacks (SYN Flood, Reset, Hijacking)
4. Week 4: Web Architecture and Cross-Site Scripting (XSS)
5. Week 5: SQL Injection and Cross-Site Request Forgery (CSRF)
6. Week 6: Clickjacking, Shellshock, and Reverse Shells
7. Week 7: User and Group Management, File Permissions, SUID/SGID Programs
8. Week 8: Environment Variables, Buffer Overflow, and Stack Overflow
9. Week 9: Return-Oriented Programming (ROP), Format String Attacks, Race Conditions
10. Week 10: Hardware Security: Meltdown and Spectre Attacks
11. Week 11: Final Group Project Presentations

Computer Resources:

This course requires a 64-bit laptop (8 GB RAM min, 16 GB recommended) running macOS 12+, Windows 10/11 (WSL2), or Linux with Docker and Wireshark installed; OpenSSL and curl are required (local or via the provided tools container). Students should use personal laptops; ECE lab machines may be used when available.

Grading:

Project 1: 30%

Labs/Quizzes: 40% (best 8 out of 11 at 5% each)

Project 2 (Open-Ended): 30%

- Proposal: 5%
- Final presentation: 10%
- Final report: 15%

COURSE POLICIES

- Please complete the homework by yourself and do not copy code from others or the internet. Any answer from Chat-GPT or any other GenAI tool needs to be identified as such. Suppose your homework is identical to others or any sample code snippets online. In that case, you will receive zero scores, and UW mandates us to report it to the College of Engineering.

- You are encouraged to discuss lab and assignment content with your classmates offline and on the discussion board. However, please limit your discussion to ideas and not discuss the code. Specifically, do not copy-paste any homework answers into the discussion board.
- Students must submit assignment and project materials online by the posted due date. Throughout the quarter, we will provide you with six late-day credits for the two assignments, which you can use to submit one or both assignment without a penalty. However, if you have used all six days, each additional late day will result in a 20% penalty in the corresponding assignment.
- Students need to submit project reports and presentations on time. The project does not have any credit days. Any overdue project materials will receive a zero score.

RELIGIOUS ACCOMMODATIONS

Washington state law requires that UW develop a policy for accommodation of student absences or significant hardship due to reasons of faith or conscience, or for organized religious activities. The UW's policy, including more information about how to request an accommodation, is available at Religious Accommodations Policy (https://registrar.washington.edu/staffandfaculty/religious-accommodations-policy/). Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form (https://registrar.washington.edu/students/religious-accommodations-request/).

ACCOMMODATIONS AND ACCESS

If you have already established accommodations with Disability Resources for Students (DRS), please communicate your approved accommodations to me at your earliest convenience so we can discuss your needs in this course. If you have not yet established services through DRS, but have a temporary health condition or permanent disability that requires accommodations (conditions include but not limited to; mental health, attention-related, learning, vision, hearing, physical or health impacts), you are welcome to contact DRS at 206-543-8924 or uwdrs@uw.edu or disability.uw.edu. DRS offers resources and coordinates reasonable accommodations for students with disabilities and/or temporary health conditions. Reasonable accommodations are established through an interactive process between the student, instructor, and DRS. It is the policy and practice of the University of Washington to create inclusive and accessible learning environments consistent with federal and state law.

ACADEMIC INTEGRITY

Engineering is a profession demanding a high level of personal honesty, integrity and responsibility. Therefore, it is essential that engineering students, in fulfillment of their academic requirements and in preparation to enter the engineering profession, adhere to the College of Engineering Statement of Principles. Any student in this course suspected of academic misconduct (e.g., cheating, plagiarism, or falsification) will be reported to the College of Engineering Dean's Office and the University's Office of Community Standards and Student Conduct to initiate the student conduct process.

TITLE IX

"UW, through numerous policies, prohibits sex- and gender-based violence and harassment, and we expect students, faculty, and staff to act professionally and respectfully in all work, learning, and research environments. For support, resources, and reporting options related to sex- and gender-based violence or harassment, visit UW Title IX's webpage (https://www.washington.edu/titleix/), specifically the Know Your Rights & Resources guide (https://www.washington.edu/titleix/files/2020/08/KYRR-guide-8-10-2020-LINKED.pdf).

If you choose to disclose information to me about sex- or gender-based violence or harassment, I will connect you (or the person who experienced the conduct) with resources and individuals who can best provide support and options. You can also access those resources directly:

- Confidential: Confidential advocates (https://www.washington.edu/sexualassault/support/advocacy/) will not share information with others unless given express permission by the person who has experienced the harm or when required by law.
- Private and/or anonymous: SafeCampus (https://www.washington.edu/safecampus/) provides consultation and support and can connect you with additional resources if you want them. You can contact SafeCampus anonymously or share limited information when you call

Please note that some senior leaders and other specified employees have been identified as "Officials Required to Report." (https://www.washington.edu/titleix/title-ix-officials-required-to-report/) If an Official Required to Report learns of possible sex- or gender-based violence or harassment, they are required to call SafeCampus and report all the details they have in order to ensure that the person who experienced harm is offered support and reporting options (https://www.washington.edu/titleix/resources/)."