CSC 600: Seminar in Computer Security

Dr. Si Chen

Spring 2025

Office:	*(25 University Ave. Room 131)*
Department Phone:	*(610-436-6998)*
E-mail:	`schen@wcupa.edu`
Class Website:	**[Link]**
Office Hours:	Monday 10:00 AM - 12:00 PM
	Wednesday 10:00 AM - 12:00 PM
	Thursday 12:15 PM - 1:15 PM
Course Mode of Instruction:	In-person (Face-to-Face)
Time and Location:	*(M 19:15 - 22:00 PM, 25 University Ave. Room 125)*

Catalog Information and Course Description

Official Course Name and Number: CSC 600: Seminar in Computer Security

This course aims to provide a comprehensive understanding of the context and foundational principles of security research and practice. We begin by exploring key questions such as the reasons for the success or failure of certain security technologies, how to measure security and assess risk, and the economics of security. Additionally, we will study various recent attacks to understand an attacker's mindset, helping students develop a well-rounded view of security research.

Building on this foundation, we will delve into state-of-the-art research and current activities in various areas of computer security, including software security, web security, security and privacy issues in cloud computing, mobile devices and networks, and IoT devices and systems. We will discuss how to define and address security research questions in these settings, exploring new threats emerging from AR/VR, cloud, mobile platforms, and IoT and Blockchain systems. The course also covers analysis techniques and tools for vulnerability discovery and threat analysis, as well as approaches for building stronger security into these platforms and applications.

This seminar is ideal for graduate students (or accelerated undergraduates) interested in current research activities and conducting research projects in computer security. By the end, participants will have a comprehensive understanding of advanced security research and will be ready to undertake their own investigations.

Enrollment Requirements:

- No formal prerequisites for graduate students (security background recommended).
- Accelerated undergraduates should have completed CSC 302 or consult with instructor.

Credits: 3

Required Hardware & Software

- A modern OS (Windows, Mac, or Linux) capable of running IDA Free and VirtualBox.
- Access to Dr. Si Chen's BadgerCTF server via Remote Desktop or SSH (credentials will be provided).

Textbook and References

Reference Books

- Randal E. Bryant, David R. O'Hallaron, *Computer Systems: A Programmer's Perspective*, 3rd Edition, ISBN 978-0134092669
- Wenliang Du, *Computer Security: A Hands-on Approach*, ISBN 978-1548367947

Additional readings and materials will be posted on our class website or D2L.

Topics Outline and Tentative Schedule

Class	Topic	Activities/Notes
1	Introduction	–
2	IA-32 Register, Byte Ordering	–
3	X86 Assembly & Stack	–
4	Stack & Stack Frame	–
5	Stack Frame & Calling Convention	–
6	System Call & Shellcode & Stack Overflow	Lab1
7	Group Presentations	–
8	CVE-2006-3439	Lab2
9	Web Security	–
10	CVE-2008-4250	Lab3
11	SQL Injection	–
12	CVE-2016-7103	–
13	Kernel Rootkit & Forensics; Volatility; Stuxnet	–
14	Final Project Work / Volatility & Stuxnet	–
15	Group Presentations	–

Additional topics include:

- Risk assessment and the economics of cybersecurity
- Assembly language concepts for IA-32 processors and stack operations
- Software exploits (e.g., DLL Injection)
- Methods for Static Analysis (PE format, etc.)
- Dynamic Analysis approaches
- Hooking techniques, including IAT hooks
- Anti-virus Software design and efficacy
- Heuristics in malware detection / Dynamic Heuristic Analysis
- Use of API Hooks for monitoring/altering system behavior
- Concepts and detection strategies for Rootkits

Programming Language & Tools

The primary languages are **Assembly** and **Python**. You will develop various security-analysis programs and scripts, with all deliverables submitted via D2L.

Grading Policy and Evaluation

Letter Grade Scale (Graduate):
A [90–100], B [80–89], C [70–79], D [60–69], F [0–59]

Component	Percentage	Details
Attendance	10%	Participation and engagement
Labs	30%	3 Malware/security analysis labs
Group Presentations	30%	2 Presentations on selected papers/case studies
Group Project	30%	1 Research project on a selected topic

Note: No credit for unexcused late assignments.

Note: At least one major evaluation will be completed, graded, and returned before the withdrawal deadline.

Course Policies

Excused Absences Policy

Students are advised to carefully read and comply with the WCU Excused Absences Policy, including absences for university-sanctioned events, in the WCU Graduate Catalog. The “responsibility for meeting academic requirements rests with the student,” and no policy excuses students from required work. Professors may require a fair alternative to in-person attendance for sanctioned absences.

Late Assignments Policy

Late assignments will be accepted with **no penalty** *only* if a valid excuse is communicated to the instructor **before the deadline**. No credit for unexcused late assignments.

Program Learning Outcomes (PLOs) and ABET Outcomes

Although this is a graduate-level course, if you are part of a combined or accelerated program, the following (undergraduate) PLOs and ABET outcomes may apply:

- **(a)** Ability to apply knowledge of computing/mathematics appropriate to the discipline
- **(d)** Ability to function effectively in teams
- **(i)** Ability to use current techniques, skills, and tools necessary for computing practices
- **(n)** Proficiency in the latest, cutting-edge technology

ABET-Specific Outcomes (relevant for undergrad track):

- **ABET-1**: Analyze a complex computing program and apply principles of computing and other disciplines to identify solutions
- **ABET-2**: Design, implement, and evaluate a computing-based solution to meet requirements
- **ABET-5**: Function effectively as a member or leader of a team

Course Outcomes (CO)

Upon completing this graduate seminar, students will be able to:

- Perform static/dynamic analysis of system malware. (Labs 1, 2, 3)
- Build or evaluate anti-malware solutions. (Lab activities, group project)
- Use forensics tools (e.g., Volatility) to analyze kernel-level rootkits. (Final project)
- Understand how to mitigate real-world malware/security attacks. (Labs, group presentations)

Accommodations for Disabilities

If you have a disability that requires accommodations under the Americans with Disabilities Act (ADA), please bring me your official letter of accommodations as soon as possible. For more information on WCU's services for students with disabilities, call 610-436-3217 or visit www.wcupa.edu/ussss/ossd.

Academic Integrity and Honesty

The Computer Science Department enforces strict policies regarding academic dishonesty:

- A student cheating on an assignment: first offense = zero for that assignment; second offense = F for the course.
- A student cheating on a test: automatic F in the course.
- Cheating includes plagiarism, unauthorized materials, impersonation, etc.

About ChatGPT and Other LLM Tools

At present (2025), the use of ChatGPT and similar AI tools is permitted for enhancing lab reports, project write-ups, and presentation slides. However, specialized analysis (disassembly, reverse engineering) requires dedicated security tools. ChatGPT cannot replace them.

Excused Absences Policy for University-Sanctioned Events

Students participating in official WCU-sanctioned events (band, NCAA athletics, etc.) will be granted excused absences for those class sessions, with the possibility of taking exams/quizzes at an alternative time. Students must present documentation on WCU letterhead, signed by the activity director or coach, prior to the missed date. All other points of the official WCU policy apply.

Reporting Incidents of Sexual Violence

Faculty are required to report incidents of sexual violence shared by students to the Title IX Coordinator (except if disclosed in a classroom discussion, writing assignment, or University-approved research project). For details, see WCU's Office of Social Equity website.

Emergency Preparedness

All students are encouraged to sign up for **WCU ALERT** (wcupa.edu/wcualert). In an emergency, call Public Safety at 610-436-3311.

Electronic Mail Policy

All official course communications will be sent via your WCU e-mail account. You are responsible for accessing and reading these communications.

APSCUF

I am a member of APSCUF (Association of Pennsylvania State College and University Faculties). We uphold the highest standards of teaching, scholarly inquiry, and service.

Final Notes

This graduate seminar follows the official WCU Final Exam schedule for Spring 2025. If no written exam is given, our final meeting slot may be used for project presentations. Any other policies not explicitly mentioned here can be found in the **WCU Graduate Catalog**.