

CSC 583: Topics in Computer Security

Dr. Si Chen

Fall 2024

E-mail: schen@wcupa.edu

Class Website: [\[Link\]](#)

Office Hours: MWF 11:50 AM – 12: 50 PM

Office: 25 University Ave, Room 131

Course Description

This course offers an in-depth exploration of ARM architecture and security, with a focus on practical applications and real-world vulnerabilities. Students will gain comprehensive knowledge of ARM instruction sets, memory management, and advanced exploitation techniques.

Key Topics include:

- **ARM Instruction Set:** Detailed study of ARM assembly language, including data movement, arithmetic operations, and control flow instructions.
- **Memory Management:** Understanding of stack and heap operations, endianness, and memory layout in ARM systems.
- **Security Vulnerabilities:** In-depth analysis of common security flaws, including stack overflow, heap overflow, and return-oriented programming (ROP) attacks.
- **Exploit Development:** Hands-on experience in crafting exploits for various vulnerabilities, using both assembly and high-level languages.
- **Advanced Topics:** Introduction to kernel exploitation and analysis of complex attack vectors.

The course combines theoretical lectures with practical lab exercises, allowing students to apply their knowledge in a controlled environment. Students will work with real ARM systems, develop exploit code, and learn to identify and mitigate security risks.

Course Mode of Instruction

This course is taught in-person. All classes are held on campus in the designated classroom.

Expected Background

- Graduate Students: Completion of all four core courses is required. A strong background in security is also expected.
- Accelerated Undergraduate Students: Completion of CSC 302 is mandatory. If you have not completed this course, please consult with the instructor for eligibility.

Required Materials

No textbook is required for this course. All necessary materials will be provided through the course website.

Course Student Learning Outcomes

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

- Demonstrate a comprehensive understanding of ARM architecture and instruction set
- Analyze and exploit common security vulnerabilities in ARM-based systems
- Develop and implement advanced exploitation techniques, including ROP and heap exploitation
- Understand and apply memory management concepts in the context of system security
- Conduct basic kernel exploitation and analyze complex attack vectors
- Apply security principles to identify and mitigate risks in ARM-based systems

Evaluation & Grading

Component	Weight	Description
Attendance	10%	Regular class attendance and participation
Labs	40%	4 practical hacking labs, 10 points each
Presentations	10%	1 group presentation, 10 points
Final Project	40%	Comprehensive final capture-the-flag (CTF) lab, group project

Tentative Course Outline

- Week 1: Introduction
- Week 2-3: ARM Instruction Set (mov/mvn, add/and, str/ldr, B, BL)
- Week 4-5: Stack & Stack Frame, System Call
- Week 6-7: ARM Security: Stack Overflow
- Week 8-9: ARM Security: Return-Oriented Programming (ROP)

- Week 10-11: ARM Security: Heap Overflow
- Week 12: Kernel Exploitation
- Week 13-15: Advanced Topics and Project Work

Required Hardware

A computer with a modern OS (e.g., Windows/MacOS/Linux/FreeBSD) which can connect to the Internet. We will utilize the BadgerCTF server hosted in the CS laboratories throughout the semester. You can connect to it using Secure Shell (SSH). Credentials/Walkthroughs will be provided.

University Policies

EXCUSED ABSENCES POLICY

Students are advised to carefully read and comply with the excused absences policy, including absences for university-sanctioned events, contained in the WCU Graduate Catalog. In particular, please note that the "responsibility for meeting academic requirements rests with the student," that this policy does not excuse students from completing required academic work, and that professors can require a "fair alternative" to attendance on those days that students must be absent from class in order to participate in a University-Sanctioned Event.

ACCOMMODATIONS FOR STUDENTS WITH DISABILITIES

West Chester University is committed to providing equitable access to the full WCU experience for Golden Rams of all abilities. Students should contact the Office of Educational Accessibility (OEA) to establish accommodations if they have had accommodations in the past or if they believe they may be eligible for accommodations due to a disability, whether or not it may be readily apparent. There is no deadline for disclosing to OEA or for requesting to use approved accommodations in a given course. However, accommodations can only be applied to future assignments or exams; that is, they can't be applied retroactively. Please share your letter from OEA as soon as possible so that we can discuss accommodations. If you have concerns related to disability discrimination, please contact the university's ADA Coordinator in the Office of Diversity, Equity, and Inclusion or 610-436-2433.

ACADEMIC & PERSONAL INTEGRITY

It is the responsibility of each student to adhere to the university's standards for academic integrity. Violations of academic integrity include any act that violates the rights of another student in academic work, that involves misrepresentation of your own work, or that disrupts the instruction of the course. Other violations include (but are not limited to): cheating on assignments or examinations; plagiarizing, which means copying any part of another's work and/or using ideas of another and presenting them as one's own without giving proper credit to the source; selling, purchasing, or exchanging of term papers; falsifying of information; and using your own work from one class to fulfill the assignment for another class without significant modification. Proof

of academic misconduct can result in the automatic failure and removal from this course. For questions regarding Academic Integrity, the No-Grade Policy, Sexual Harassment, or the Student Code of Conduct, students are encouraged to refer to the Department Graduate Handbook, the Graduate Catalog, the Ram's Eye View, and the University website.

REPORTING INCIDENTS OF SEXUAL VIOLENCE

West Chester University and its faculty are committed to assuring a safe and productive educational environment for all students. In order to comply with the requirements of Title IX of the Education Amendments of 1972 and the University's commitment to offering supportive measures in accordance with the new regulations issued under Title IX, the University requires faculty members to report incidents of sexual violence shared by students to the University's Title IX Coordinator. The only exceptions to the faculty member's reporting obligation are when incidents of sexual violence are communicated by a student during a classroom discussion, in a writing assignment for a class, or as part of a University-approved research project. Faculty members are obligated to report sexual violence or any other abuse of a student who was, or is, a child (a person under 18 years of age) when the abuse allegedly occurred to the person designated in the University Protection of Minors Policy. Information regarding the reporting of sexual violence and the resources that are available to victims of sexual violence is set forth at the webpage for the Office of Diversity, Equity and Inclusion.

INCLUSIVE LEARNING ENVIRONMENT AND ANTI-RACIST STATEMENT

Diversity, equity, and inclusion are central to West Chester University's mission as reflected in our Mission Statement, Values Statement, Vision Statement and Strategic Plan: Pathways to Student Success. We disavow racism and all actions that silence, threaten, or degrade historically marginalized groups in the U.S. We acknowledge that all members of this learning community may experience harm stemming from forms of oppression including but not limited to classism, ableism, heterosexism, sexism, Islamophobia, anti-Semitism, and xenophobia, and recognize that these forms of oppression are compounded by racism.

Our core commitment as an institution of higher education shapes our expectation for behavior within this learning community, which represents diverse individual beliefs, backgrounds, and experiences. Courteous and respectful behavior, interactions, and responses are expected from all members of the University. We must work together to make this a safe and productive learning environment for everyone. Part of this work is recognizing how race and other aspects of who we are shape our beliefs and our experiences as individuals. It is not enough to condemn acts of racism. For real, sustainable change, we must stand together as a diverse coalition against racism and oppression of any form, anywhere, at any time.

Resources for education and action are available through WCU's Office for Diversity, Equity, and Inclusion (ODEI), DEI committees within departments or colleges, the student ombudsperson, and centers on campus committed to doing this work (e.g., Dowdy Multicultural Center, Center for Women and Gender Equity, and the Center for Trans and Queer Advocacy).

EMERGENCY PREPAREDNESS

All students are encouraged to sign up for the University's free WCU ALERT service, which delivers official WCU emergency text messages directly to your cell phone. For more information, visit <http://www.wcupa.edu/wcualert/>. To report an emergency, call the Department of Public Safety at 610-436-3311.

ELECTRONIC MAIL POLICY

It is expected that faculty, staff, and students activate and maintain regular access to University provided e-mail accounts. Official university communications, including those from your instructor, will be sent through your university e-mail account. You are responsible for accessing that mail to be sure to obtain official University communications. Failure to access will not exempt individuals from the responsibilities associated with this course.