CS 468: Secure Programming and Systems
Spring 2025

Section 002: MW 1:30 pm – 2:45 pm
Location: 1200 Merten Hall

Qiang Zeng, Ph.D. Associate Professor Department of Computer Science 4448 Engineering Building **zeng@gmu.edu**	Course Websites: Blackboard https://cs.gmu.edu/~zeng/cs468-s25/
	Teaching Assistant: TBD
	Office Hours: W 10:00 am – 12:00 pm

Course Syllabus

Description

This course covers mechanisms, approaches, and techniques used for secure programming and building a secure system. Topics include security basics (e.g., cryptography, authentication, access control), threat modeling, and common attacks/threats/vulnerabilities/countermeasures. We will also discuss attacks and defenses based on recent research papers.

Prerequisites

Grade of C or better in CS310 and CS367

Textbook

None

Course Outcomes

As a result of successful participation in this course, students will be able to:

1. Understand the properties and features of various cryptography algorithms, and employ cryptographic techniques for data and communication protection
2. Distinguish different access control policies
3. Identify common attacks and their consequences
4. Define the threat model when designing a system
5. Incorporate various defense techniques to build a secure computer system
6. Analyze the advantages and disadvantages of latest security techniques

Topics

We will learn and practice methods and techniques used to analyze the threats faced by a computer system, and apply defense techniques to enhance security. In addition, we will discuss recent advances in both attack and defense techniques, and learn how to assess a security technique.

First, we will learn the most important cryptography algorithms and understand the strengths and shortcomings of each. Second, we will learn how to define the threat model for a given system. For that purpose, we need to learn the most common vulnerabilities and attacks. Third, we will discuss the most important security techniques, such as authentication and authorization, and how to employ them to build secure computer systems. Finally, we will discuss a series of latest attacks and defense techniques. In this process, we will learn how to assess a security technique in terms of its resilience, efficiency, scalability, and costs. **Web and network security will NOT be the focus.**

Attendance Policy

You are expected to attend class lectures and participate in class discussions. If you expect to miss class for any reason you should contact the instructor by email as soon as possible. You are responsible for all material covered in lectures whether you are present or not.

Lecture presentations assume that you have read the assigned material **before** coming to class and are prepared to ask questions during class. If you don't ask questions, then I will assume that you understand the material. If there is a topic you do not understand, **it is your responsibility** to seek clarification from me during lectures or during office hours, or from other students. If you miss a lecture, **it is your responsibility** to get the notes and announcements from a classmate.

Time Commitment and Planning

Any university course requires a large amount of work outside of lecture. I assume that when you register for this course you will allocate an average of at least three to four (3-4) hours per week, in addition to lectures, to read the papers, complete the course project assignment(s), and prepare for exam(s). It is your responsibility to manage your workload.

Classroom Behavior

Cell phones, PDAs, music players and other electronic devices that can distract you and other students must not be used in the classroom. Please remember to turn off the audio ringer on your cell phones before entering the classroom. Under no circumstances should you use a phone or PDA while class is in session. If your cell phone rings during class or you are involved in any other form of disruptive behavior that creates a disturbance in class (such as reading a newspaper, sleeping, texting, or having extended conversations), you may be asked to leave the classroom.

Similarly, while you may use your laptop computer during class to take notes, using your laptop in a way that distracts other students around you or otherwise disrupts the class (e.g., surfing the web, reading email, or playing audio/video recordings) is not permitted, and may result in you being asked to leave the classroom. You should plan to arrive before class begins and not leave until after class ends. This is an issue of respect for everyone involved – not just for the instructor, but also the students whom you disturb with your late entry and/or early departure. If you arrive late to (or must leave early from) a lecture please sit near an exit in the back of the classroom.

Course Format

The class will include a mixture of lectures, case discussions, and student presentations. The course is highly interactive in nature, so students are expected to come to class prepared to discuss readings.

Grading Policy

Your overall final course letter grade will be determined by your grades on the following assessments.

Project Assignment(s) One day late: 20% deduction Two days late: 40% deduction Three days late: score 0	20%
Presentation	30%
Class Discussion and Participation	10%
Midterm Exam (No Final Exam)	40%

Your final grade is based on the total points you have earned over the semester. The percentage scores are translated to letter grades as follows:

A+: >= 95%; A: [90%, 95%); A-: [85%, 90%)
B+: [80%, 85%); B: [75%, 80%); B-: [70%, 75%)
C+: [66%, 70%); C: [63%, 66%); C-: [60%, 63%)
D: [50%, 60%)
F: < 50%

Important Note Regarding Grade Appeals

Grade appeals for any assessment must be requested (either in writing or via email to me) within one (1) week of my posting the grade to Blackboard.

ACADEMIC INTEGRITY

All students must abide by the GMU Academic Standards Code and CS Department's Honor Code and Academic Integrity Policies during the semester. The students are supposed to work *individually* on the assignments. Collaboration will be allowed only for the group assignments, within each group. We reserve the right to use automated tools such as MOSS to detect plagiarism. The violations of Honor Code will be reported to GMU Academic Office without any exception. The university procedures for adjudicating such violations, including types of sanctions and GMU Sanctions Matrix can be found at the following link . All students must be familiar with the Academic Standards code, as well as Common Policies Affecting All Courses at George Mason University.

DISABILITY STATEMENT

If you have a learning or physical difference that may affect your academic work, you will need to furnish appropriate documentation to GMU Disability Resource Center. If you qualify for accommodation, the DRC staff will give you a form detailing appropriate accommodations for your instructor. If you have such a condition, you must talk to the instructor during the first week of the term about the issue.