CS468 Secure Programming and Systems

Location:	Exploratory Hall L003
Meeting Time:	Tuesday, Thursday 3:00-4:15
Instructor:	Dr. Maha Shamseddine
Office:	Buchanan Hall D215I
E-mail:	maha@gmu.edu
Office Hours:	Tuesday 10:30-12:00 or by appointment

Teaching Assistants Anish Kumar Saranga (asaranga@gmu.edu), Nikhil Dilip Dhore (ndhore@gmu.edu)

Description:

This course is designed to provide students with an understanding of the theoretical underpinnings of modern security systems, along with the principles of secure system and protocol design. This course is intended for upper-division computer science students, along with other students whom possess the required programming and system software background. Topics include security and cryptography basics, vulnerability analysis, secure software development for communications and distributed system security. Projects involve designing and programming basic security tools, secure programs, and distributed systems.

Prerequisites

Grade of C or better in CS310 and CS 367.

Required Textbook

Cryptography and Network Security: Principles and Practice, 7 or 8th edition by William Stallings.
ISBN-13: 9780134444611
Publisher: Prentice Hall

Topics

- Cryptography
- Secure Programming
- Secure Systems
- Securing Networks and Distributed Systems

Class Materials

All class materials, including lecture notes, are available through your blackboard accounts.

Homeworks

There will be several homeworks assigned throughout the semester. They will be a mixture of written questions and programs. The programs involve the design and implementation of a protocol for encrypted and authenticated secure network communication. All programs will be written in the C language.

Please NOTE

- If your code does not compile, you will get no credit.
- Assignments and Projects are individual efforts.
- We reserve the right to use MOSS to detect plagiarism.

Grading Policy

Your grade will be calcuated as follows:

- 40% Homeworks
- 5% Class participation
- 2 Midterms, 15% each
- 25% Final exam (cumulative)

No credit if your project does not compile. Homeworks are due at the start of class, not during class. Late assignments/projects lose 10% credit *per day* and will not be accepted 3 days after the due date.

No early exams will be given. If you must miss an exam an makeup will be arranged at the discretion of the instructor, provided you have a written and verified excuse. Please note: You must score a 50% or higher on the final to pass this class.

Course Outcomes

1. Describe the fundamental ethical responsibilities computer scientists have in securing and protecting computers.
2. Explain basic mathematical principles underlying encryption algorithms.
3. Explain basic mathematical principles underlying authentication algorithms.
4. Demonstrate an understanding of cryptographic protocols.
5. Demonstrate an understanding of secure programming via attack models and vulnerability analysis.
6. Describe how Operating Systems implement security for critical system components.
7. Explain network and transport level security protocols with IPSec.
8. Illustrate fundamental understanding of security principles by programming projects in cryptography, secure programming and communications.

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.

Disability Resource Center

Covid Requirements

The class requires all GMU COVID requirements be met, including *strict* masking requirements.

Honor Code

The GMU Honor Code will be *strictly* enforced. Please make sure that you are familiar with it. We will discuss this further in class. Below is the link to the code.

Honor Code