CS 499: Foundations and Advances of Cybersecurity (Fall 2024)

Department of Computer Science

George Mason University

Instructor: Dr. Xiaokuan Zhang (xiaokuan@gmu.edu)

This syllabus is tentative and subject to change

- ## Basic Information

Time:	TBD
Location:	TBD
Credits:	3
Office Hour:	TBD

- ## Recommended Textbook
  - Introduction to Computer Security, Goodrich and Tamassia, 1st edition
  - Principles of Information Security, Whitman and Mattord, 6th edition
  - Security Engineering, Anderson, 3rd edition
  - Computer Security: A Hands-on Approach, Du, 3rd edition

- ## Course Description

  This course provides an introduction to foundational topics of information security. We will cover various topics, including a brief introduction to cryptography, network security, operating systems security, software security, web security, etc. We will also introduce the most recent advances in security.

- ## Course Format

  This course will consist of a combination of lectures, hands-on labs and discussions on recent security research papers. Students will have the opportunity to get hands-on experiences on real-world security problems and gain practical experience.

- ## Course Objectives

  - Learn key concepts and terminology in cybersecurity.
  - Obtain basic knowledges in different areas of cybersecurity.
  - Identify threats to cybersecurity in different scenarios.
  - Learn about strategies to identify and remediate vulnerabilities in software and systems.
  - Understand the recent advances in cybersecurity.

- Obtain hands-on experiences on cybersecurity projects.

- **Prerequisites**

  - Have basic understanding of math concepts, such as probability;
  - Have a good understanding of data structures and algorithms;
  - Comfortable writing programs from scratch in C and Java;
  - Comfortable in a command-line Unix development environment (gdb, gcc, etc);
  - Have basic knowledge of assembly languages such as x86.

  Course prerequisite requirement:
  - **Required** pre-requisite: CS310, CS330
  - **Recommended** pre-requisite: CS367, CS471

  Device requirement: Students need to have a laptop/computer that can run Linux systems such as Ubuntu (for Windows/Mac users, you can run ubuntu on Virtual Machines).

- **Grading Policy**

  Participation: 5%
  Programming Labs: 40%
  Research paper review + discussion: 20%
  Research Projects: 35%

  The final grade is computed based on the following rules:
  A+ (>= 95.0%) A (>= 90.0%) A– (>= 85.0%)
  B+ (>= 80.0%) B (>= 75.0%) B– (>= 70.0%)
  C+ (>= 66.0%) C (>= 63.0%) C– (>= 60.0%)
  F (< 60.0%)

- **Topics (Tentative)**

  - Cryptography Basics
  - Network Security
  - Software Security
  - Web Security
  - Side-channel Security
  - Operating System Security
  - Mobile Security
  - Authentication and Access Control
  - Privacy

- Security of Emerging Technologies (AI, web3, VR, etc.)

- **Late Policy (for homework/project)**

  Late submissions receive partial credit:

  - Late for no more than 4 hours: 90% of credit
  - Late for more than 4 hours but no more than 12 hours: 75% of credit
  - Late for more than 12 hours but no more than 24 hours: 50% of credit
  - Late for more than 24 hours but no more than 48 hours: 25% of credit
  - **Late for more than 48 hours: no credit**

- **Email Policy**

  The instructor can be reached at xiaokuan@gmu.edu. Please include **[CS 499]** in the subject line of emails for prompt response. Students must use their GMU email account to receive important University information, including communications related to this course. The instructor cannot respond to messages sent from or send messages to a non-Mason email address. To protect your privacy, the instructor cannot list your GMU email address on any public forum or provide it to any other students. You may, of course, give your email address to any other students.

- **Honor Code**

  Please see the Office for Academic Integrity (https://oai.gmu.edu/) for a full description of the code and the honor committee process, and the Honor Code Policies of the Department of Computer Science (https://cs.gmu.edu/resources/honor-code/) regarding the course project. GMU is an Honor Code university. The principle of academic integrity is taken seriously and violations are treated gravely. If you rely on someone else's work in an aspect of the course project, you should give full credit in the proper, accepted form. Another aspect of academic integrity is the free play of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions. When in doubt (of any kind) please ask for guidance and clarification.

- **Inclusion**

  Every student in this course is exactly where they belong and it is our honor to welcome each of you to join us in learning throughout this semester. Every student in this course, regardless of background, sex, gender, race, ethnicity, class, political affiliation, physical or mental ability, veteran status, nationality, or any other identity category, is an equal member of our course. You have the right to be called by whatever name you wish, to be

referred to by whatever pronoun you identify, and to adjust these at any point. If you feel uncomfortable in any aspect of our instruction that results in any barrier to your inclusion in this course, please contact the instructor directly.

- **Disabilities**
  Students with a disability or other condition (documented with GMU's Office of Disability Services, ODS) that may impact academic performance should speak with the instructor as soon as possible to discuss appropriate accommodations. If you are in a situation that even temporarily affects your ability to learn or work, such as with a broken limb or other such injury, contact the Office of Disability Services to get accommodations. The instructor is happy to assist as is appropriate, but it must be documented ahead of time by ODS. Even if you do not know if you plan on utilizing the accommodations, it is in your best interest to prepare them in advance.

- **Sexual Harassment and Interpersonal Violence**
  As a faculty member and designated "Responsible Employee," the instructor is required to report all disclosures of sexual assault, interpersonal violence, and stalking to Mason's Title IX Coordinator per university policy 1412. If you wish to speak with someone confidentially, please contact the Student Support and Advocacy Center (703-380-1434), Counseling and Psychological Services (703-993-2380), Student Health Services, or Mason's Title IX Coordinator (703-993-8730, cde@gmu.edu).

- **Privacy**
  Video recordings of class meetings that are shared only with the instructors and students officially enrolled in a class do not violate FERPA or any other privacy expectation. All course materials posted to Blackboard or other course site are private; by federal law, any materials that identify specific students (via their name, voice, or image) must not be shared with anyone not enrolled in this class.

- **Use of Generative AI (Gen-AI)**
  ChatGPT or other Generative-AI models may be used (but not encouraged) in this course as an assistant when working on programming assignments or projects; students may use chatGPT as an alternative to searching for debugging assistance, similar to websites such as StackOverflow.

Any use of Gen-AI models must follow the fundamental principles of the Honor Code and include the following statement with project submission:

The ideas in this submission are original and were generated by (*my name*). ChatGPT (*or name other Generative-AI model*) was used as an editorial/coding assistant, however, I take full responsibility for the originality and accuracy of the content.

However, for any writing assignments such as paper reviews or project reports, the use of Gen-AI models is strictly forbidden, mainly because 1) Gen-AI cannot really understand papers; 2) using Gen-AI to generate reviews without reading the paper can constitute "cheating".

Risk accompanies the use of any powerful tool. Students are cautioned that sharing their original ideas with Generative-AI models can lead to a loss of control and ownership of those ideas and coding. Furthermore, in terms of learning in this class, students who replace their own learning and project work with materials prepared by Gen-AI models:

- Surrender control over the material's truthfulness and accuracy and violate the university's Honor Code.
- Sacrifice the opportunity to acquire the knowledge, skills, and critical thinking taught in the course.
- Risk being unable to perform to expectations when Gen-AI models are unavailable, such as in exams or interviews.
- Ultimately endanger their employability if they are unable to produce work other than that produced by Gen-AI models.