CS 795: Security Issues on Emerging Computer Systems (Fall 2023)

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 & Location:	Thursday 7:20-10:00pm ET
Location:	Horizon Hall 1011
Credits:	3
Textbook:	None
Office Hour:	By Appointment

- **Course Description**

  Computer systems are constantly evolving to meet the diverse needs of the users. Recently many new systems have emerged and changed the world, such as blockchain, cryptocurrency, virtual reality, confidential computing, etc. In this course, we will discuss the recent advances in these emerging computer systems, especially their security issues. Students will be expected to read, evaluate, and discuss research papers selected from top-tier security conferences such as IEEE S&P, ACM CCS, USENIX Security, NDSS, and top system conferences such as OSDI, SOSP.

- **Course Format**

  In most lectures, we will discuss a particular topic of Security. First, the instructor will give a brief overview of the selected topic. Then, students will give two presentations of two selected research papers, and other students will raise questions. Finally, we will discuss the papers in terms of strength/weakness and brainstorm new research ideas. Some part of the lectures will be allocated for your project presentation, including proposal, mid-term status report, and final project presentation. In addition, we may have up to two guest lectures.

- **Prerequisites**

Students should have maturity in both the mathematics of computer science and in the engineering of computer systems. This means that Students should: have a good understanding of data structures and algorithms; be comfortable writing programs from scratch in C and Java; and be comfortable in a command-line Unix development environment (gdb, gcc, etc). Students should also have a good understanding of computer architecture, operating systems, and computer networks. Knowledge of assembly languages such as x86 is strongly preferred. Most importantly, Students should be eager to challenge themselves and learn more!

Prerequisite requirement: **Operating Systems (CS 571) or Computer Networks (CS 555) or Cryptography (CS 587) or the permission of the instructor**.

- **Topics (tentative)**
  - Blockchain/Smart Contract Security
  - Side-channel Attacks and Defenses (e.g., Spectre and Meltdown)
  - Trusted Execution Environments (TEEs) and Confidential Computing
  - Mobile Security (e.g., Android/iOS)
  - Security of Mixed Reality Platforms (e.g., Oculus Quest)

- **Your Responsibilities (there are no midterm or final exams)**

  1. Read two assigned papers before each lecture and submit your critiques
  2. Give presentations of selected papers from a reading list (the frequency depends on the size of the class)
  3. Lead discussion on presented papers
  4. Conduct a team project (three key deadlines: proposal, status report, and final report)

- **Paper Critique**

  The critique, within a one-page limit (~500 words), must be submitted electronically through Blackboard by 11:59pm ET on Wednesday every week. **Please do not email the instructor your paper critique.** The papers that are required to read will be posted on Blackboard. A good critique should include the following:

  1. What is the problem that the paper aims to solve?
  2. What is the high-level approach used?
  3. What are the key motivations, observations, and results?
  4. How does this work advance the state-of-the-art? (strength?)
  5. What are the limitations of the proposed work? (weakness?)
  6. What is the potential future work enabled by this paper?

If you miss more than 50% of the reviews/critiques, you will FAIL.

- **Project**

  The project is a key component of this course. The list of suggested project ideas will be posted on Blackboard. You can also develop your own project idea. The project could be open-ended explorations to some extent. Team projects with at most two students, especially multi-disciplinary collaborations, are encouraged. Individual projects are also allowed for this course. The project can be either implementation/evaluation based or a survey paper. To keep good progress, three documents must be submitted before their deadlines. For a team project, the whole team must submit one unified version of each document (instead of having each member submitting his/her own). The due dates will be announced on Blackboard.

  1. Project Proposal (2 pages in single-column 11-point format)
  2. Status Report (2 pages in single-column 11-point format)
  3. Final Report (at least 5 pages in double-column 10-point ACM format, excluding refs)

  LaTeX and Microsoft Word templates for the final project report will be available on Blackboard.

- **Late Policy**

  Late submissions of paper critique receive no credit.

  Late submissions of project reports receive partial credit:

  - Late for no more than 24 hours: 80% of credit
  - Late for more than 24 hours but no more than 48 hours: 60% of credit
  - **Late for more than 48 hours: no credit**

- **Grading Policy**

  Project: 40% (Proposal: 10%, Status Report: 10%, Final Report: 20%)
  Paper Presentation: 20%
  Paper Summary: 20%
  Participation: 20%

  The final grade is computed based on the following rules:
  A+: >= 95%; A: [90%, 95%); A-: [86%, 90%)
  B+: [84%, 86%); B: [82%, 84%); B-: [80%, 82%)
  C+: [76%, 80%); C: [73%, 76%); C-: [70%, 73%)
  D+: [66%, 70%); D: [63%, 66%); D-: [60%, 63%)

F: < 60%

- **Email Policy**

  The instructor can be reached at xiaokuan@gmu.edu. Please include **[CS 795]** 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.