George Mason University
College of Engineering and Computing

ISA 673: Operating Systems Security
Fall 2022

Section 001: Friday 1:30 pm – 4:10 pm
Location: Horizon Hall 1010

Qiang Zeng, Ph.D. Associate Professor Department of Computer Science Research Hall 356 Email: qzeng2@gmu.edu Homepage: cs.gmu.edu/~qzeng2	Course Websites: mymasonportal.gmu.edu/ (grades and materials) https://cs.gmu.edu/~qzeng2/isa673-f22 (schedule)
	Teaching Assistant: None
	Office Hours: TR 10:30 am – 11:30 pm, or by appointment

Course Syllabus

Course Description

The objective of this course is to provide an in-depth introduction to the security issues - including vulnerabilities, threats, exploits and defense mechanisms in operating systems. Topics covered include auditing, address space randomization, memory protection, virtual machine introspection (VMI), malware, etc. The course emphasizes on real world vulnerabilities (e.g., buffer overflow), threats, exploits (e.g., gaining remote shell) and defense (e.g., malware detection, analysis). In addition, the course brings the state of the art of operating system security to students and expose them to open problems (e.g., rootkit, malware defense) in operating systems security.

Clarification: This is not a hacking course.

Learning Outcomes

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

1. Knowledge of the state of the art of operating systems security.
2. First-hand experience in operating systems security.
3. Deep understanding on security vulnerabilities, exploits and defense, as well as the technical challenges and fundamental limitations of existing operating system security solutions.

Prerequisites

CS 571 and ISA 562; or permission by the instructor.

The students are expected to have good understanding on Unix/BSD/Linux operating system internals (e.g. system call internals, run-time memory organization, assembly language of x86). Proficiency in C programming is essential to successes in the course projects.

Textbook and Readings

There is NO textbook for this course. The course is based on current research papers and technical reports!

Reference Books

- *Professional Linux Kernel Architecture*, Wolfgang Mauerer.
- *Understanding the Linux Kernel, Third Edition*, Daniel P. Bovet and Marco Cesati.

Class Schedule

Please check here: https://cs.gmu.edu/~qzeng2/isa673-f22

Class schedule is tentative and subject to change. Please check frequently.

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 course materials and papers, complete the course project assignments, and prepare for exams. 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.

Assessments

There will be NO written exams ☺

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

Project Assignments – Two projects, each 15%	30%
Paper Presentations (each student presents two papers)	20%
Research Assignment and Presentation	40%
Class Discussion and Participation	10%

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:

The final grade is computed according to the following rules:

- 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+: [56%, 60%); D:[53%, 56%); D-: [50%, 53%)
- 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.

Summary of Assessments

- **Project Assignments:** You will be required to turn in project assignments **via Blackboard** on time.

- **Paper Presentation**: Each of you will be required to prepare two in-class presentations (30 minutes each) based on recently published OS Security papers. The grading will be mainly based on how well you present *research motivation, problem definition, ideas, techniques, and limitations of the work.* Critical thinking and deep insights into the research work are important to get a good score.

- **Research Assignment and Presentation:** You will have two options. (1) Reproducing the results of a paper on OS Security published in Big Four (Oakland, CCS, USENIX Security and NDSS), OSDI, SOSP or ASPLOS, pointing out a limitation of the work (we need to discuss this before you proceed, as we do not want it to be too trivial or too ambitious), and fixing the limitation. You will have chance to earn up to 20 points over your final weighted grade if you make scientific contributions (e.g., if you are not excellent in paper presentation, you may want to consider this option and earn bonus points). You need to present your work and demo it in class. (2) Selecting a recent "hot" topic about OS Security, reading 5-10 recent papers, getting systematic and deep understanding, writing a lot of slides demonstrating your good understanding, and presenting it in 1 hour. I suggest you start with a SoK (Systematization of Knowledge) paper, but reading a SoK papers is far from sufficient. If you do not demonstrate systematic and deep understanding and cannot answer my questions, you cannot earn a great score.

  Both need you to submit a report of 5-10 pages. You need to share the report with the class before the presentation. This will be a group task, with each group having two students. You can also choose to solo, and I will lower my expectation accordingly.

Request for Accommodations

If you have a documented learning disability or other condition that may affect academic performance you should: 1) make sure this documentation is on file with the Office of Disability Services (SUB I, Rm. 222; 703-993-2474; www.gmu.edu/student/drc) to determine the accommodations you need; and 2) talk with me to discuss your accommodation needs. All academic accommodations must be arranged through the ODS.

Academic Integrity

All students are required to follow all university (https://oai.gmu.edu/mason-honor-code/), school and department (https://cs.gmu.edu/resources/honor-code/) policies regarding academic integrity. Violator of the Honor Code will result in a grade of F for the course, as well as any penalties imposed by the university and/or the CS department.

Academic Integrity

The course contains materials provided by Dr. Xinyuan Wang.