CPR E 440: Operating System Security

Fall 2024

Instructor: Yong Guan
Office: 309 Durham Hall, ECE Dept.
Iowa State University
Ames, Iowa 50011

Tel: (515) 294-8378(o)
Fax: (515) 294-8432
E-mail: yguan@iastate.edu
http://www.eng.iastate.edu/∼guan/

Course Description:

OS is the core for all of todays increasingly diverse and complex computing ecosystem, which extends from smart things, personal devices, enterprise-level systems, to (micro-)service-oriented applications, with many processing increasingly carried in the cloud. Securing OS has become the most critical task for everyone and business sectors, in a variety of application contexts.

The course will focus on both the fundamentals and advanced topics in operating system security, and teach the students the design issues, principles, mechanisms, and good engineering practice for design and implementation of secure computer/OS systems. Lectures cover threat models, vulnerabilities, attacks compromise security, and advanced OS-level techniques for achieving security. Topics include OS security concepts and principles, seminal security in Multics, vulnerabilities in ordinary systems, secure capability systems, information flow control, mandatory access control, security kernels, memory protection, file system, virtual machine systems, hardware/architecture support (e.g., Intel SGX) for OS security, secure microkernel OSes (e.g., seL4, QNX, Fuchsia), modern mobile operating systems (e.g., Android and iOS), and security from end-user perspective. Assignments include labs exploring and implementing the technologies in the context of the Linux, Android, seL4/QNX/Fuchsia systems (some involving kernel programming).

One of this year's theme is on secure microkernel OSes (seL4, QNX, and Google Fuchsia). Through the course, you will get a chance to learn and work with the latest developments around them.

Prerequisite:

Prerequisites: CPR E 308 OR COM S 352. Familiarity with operating system concepts, and assume the knowledge of C programming.

Course Materials:

We will use a set of selected seminal and recent OS security papers, in addition to the following required textbook:

- Book: Operating System Security (Synthesis Lectures on Information Security, Privacy, and Trust), by Trent Jaeger. ISBN: 9781598292121, 1598292129.
- Digital copy (via ISU netid, free?): An online version is available at
  https://www.morganclaypool.com/doi/pdf/10.2200/S00126ED1V01Y200808SPT001.
  or https://link.springer.com/content/pdf/10.1007/978-3-031-02333-0.pdf

The following is a list of reference (recommended, but not required) books:

- Modern Operating Systems, by Andrew S. Tanenbaum, 4th Edition
- Operating Systems: Principles and Practice, by Thomas Anderson and Michael Dahlin.
- Fundamentals of Secure Computer Systems, by Brett Tjaden.
- Security Engineering: A Guide to Building Dependable Distributed Systems, by Ross Anderson, 3rd(/2nd/1st) Edition. Online versions for the 2nd edition is available at https://www.cl.cam.ac.uk/ rja14/book.html.

Course Outline:

- Course Overview. What is a secure OS?

- Parts of an OS: kernel and modules
- Vulnerabilities and threats
- Lessons learned from Multics
- Security kernels
- Integrity models
- Information flow control
- Secure handling of Processes & Threads, Concurrency
- Secure memory management
- Secure file systems
- Secure communication and messaging
- Hardware/Architecture support for OS security (SGX and attacking SGX)
- Virtual machine systems
- Case Study: Linux security modules and SELinux
- Case Study: Android OS security
- Case Study: seL4 and QNX
- Untrusted OS
- OS support for Application, IoT and Cloud Security

Grading:

Grading will be on the absolute scale. The cutoff for an 'A' will be at most 90% of total score, 80% for a 'B', 70% for a 'C', and 60% for a 'D'. However, these cutoffs might be lowered at the end of the semester to accommodate the actual distribution of grades.

1. Mid-term & and optional Final Take-home Exam (We choose the best one of the two): 30%
2. Course Projects: 30%
3. Online quizzes: 15%
4. Term Paper (Short surveys on selected OS security topics): 10%
   (a) Vision and Related Work: Give your view of the big picture and compare and relate the work with each other, on the topic selected by each student.
   (b) Critiques: Identify holes, research questions, and potential improvements of the work.
   (c) Depth and breadth of the knowledge in the materials
5. Term Paper Presentation: 5%.
6. Micro-kernel OS case studies, demos/presentations, and investigative analysis: 10%

Academic Policy:

1. All incidents of academic dishonesty will be dealt with according to the university policy. No exceptions.

(a) All references must be properly cited, including internet web pages (URL must be provided). If plagiarism is detected, i.e. without proper citation and quotation, you will automatically receive an F. When in doubt, please ask the instructor if it is reasonable to include other's work in your assignments.

2. We welcome and highly encourage students' active class participation and discussions.

3. Due date for all the assignments is hard (no late hand-in will be accepted.) except that you have reasonable reasons. However, for the whole semester, you may have at most one time no-reason three-day extension. But the due dates in the dead week are firm (no extension).

Free Expression

Iowa State University supports and upholds the First Amendment protection of freedom of speech and the principle of academic freedom in order to foster a learning environment where open inquiry and the vigorous debate of a diversity of ideas are encouraged. Students will not be penalized for the content or viewpoints of their speech as long as student expression in a class context is germane to the subject matter of the class and conveyed in an appropriate manner.

More details about the statement can be found at **https://www.celt.iastate.edu/teaching/preparing-to-teach/how-to-create-an-effective-syllabus/recommended-iowa-state-university-syllabus-statements/**

Time: Tuesday & Thursday 11 am - 12:15 pm

Location: Howe 1242.

Online Zoom office Hours: Thursday 2-3pm. You are welcome to join via the following Zoom link, or email me a time to schedule a meeting:

https://iastate.zoom.us/j/92372099753?pwd=cXdGME92THVFTlZDMlZLK3cwUDc3Zz09