W211 Operating System Security Syllabus

UC Berkeley School of Information
Master of Information and Cybersecurity

Course Description

This survey of operating system security will compare approaches taken among several modern OSs and how to conceptualize design issues, principles, and good practices in securing systems in today's overall computing ecosystem, which extends from things and personal devices to enterprises increasingly in the cloud. Practitioners seldom have the luxury (or even the ability) to choose the OS that best fits some complex and evolving situations. In established enterprises, they have to manage more than *nix and Windows—people want to work with their own devices, too. And securing a single machine is different from securing a rack full—or a datacenter full—of machines, many of which will be virtual, containerized, or in some cloud service.

I've found operating systems to be of great interest over many years, both philosophically and practically. But frustrating, too! (Why the devil did they do it that way? What could they have been thinking? How is anyone supposed to understand and use that feature or write a program to reliably use it? Why didn't they ship the system to be more secure in the first place?)

The purpose of this course is to equip you to think about and address challenging issues and problems involving operating system security in the kinds of diverse environments you will inevitably run into in actual enterprises, even if you're lucky enough to start from scratch. These are typically situations where you need to make different OSs play well together.

We'll start with the history of OSs and OS security from the beginning of (OS) time, covering lessons learned (and subsequently forgotten) and the security "special features" of modern OS contenders. When they are not particularly "special" as they come out of the box, we'll cover how to enhance them by configuration or adding (mostly free) software alongside.

Learning Objectives

By the end of the course, the student will be able to

- Appraise installed systems for their security, confidentiality, and integrity characteristics
- Diagnose and recover from typical security problems on a variety of operating systems (e.g., malware, rootkits)
- Solve problems typically presented to security practitioners in regular work practices

- Examine and verify system configurations for their adherence to security policies
- Modify systems to enhance security and auditability by reconfiguring and adding open source components
- Compare operating system alternatives and free software enhancements based on business needs and the corresponding security properties
- Perform a root-cause analysis of security failure
- Search effectively for many kinds of security-related information on the Internet

Course Assignments and Assessment

- 20%: Participation (collaboration within your groups and class discussion)
- 20%: Individual written reflections on readings/viewings of supplementary papers and presentations)
- 60%: Labs (A mix of projects, software evaluations, forensic analysis exercises)

Written assignments will include brief analysis of papers, questions involving performing online research, and discovery and evaluation of software alternatives to address some typical problems.

Prerequisites

- This course assumes you have working knowledge of computer systems organization and the basics of UNIX programming.
- You should be comfortable operating some OS at the command line (not GUI) level.
- You must know how to install an OS from scratch in a virtual machine.
- You must know how to boot Linux distributions from external media (such as a USB stick).

Understanding of OS internals is a benefit, but not required. Additional non-credit sessions will be available throughout the semester to cover OS fundamentals.

Technical Resources

- You need a working computer running modern Windows, Linux, or Mac OS X.
- We will all need to use headphones with a separate microphone usable with the zoom client on your computer for the live sessions (i.e. the built-in speakers and microphone on your computer will almost certainly not be suitable.)
- (While buying hardware, you will likely need disk space for this course for downloaded software, OS and VMdisk images if you want to run the labs exercises locally.)

Recommended Texts

These are books which will be generally useful for the course (and you ought to have them in your professional library, anyway):

Ross Anderson, Security Engineering
The second edition and bits of the forthcoming third edition (as they are written) are online here:
https://www.cl.cam.ac.uk/~rja14/book.html

Peter Guttmann, Security
https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf

Steve Bellovin, Thinking Security
https://proquest.safaribooksonline.com/book/networking/security/9780134278223

Instructor Biographies

Matthew Garrett

mjg59@berkeley.edu

Matthew is a security developer at Aurora, and formerly worked at companies such as Google, CoreOS and Red Hat. He has an extensive background in OS, firmware and hardware security, and the interactions between each of these.

George Neville-Neil

gnn@neville-neil.com

Nathan Freitas

Nathan Ide