EC 521: CyberSecurity, Spring 2018

Instructor

Manuel Egele

For correspondence, post to the piazza course site

Office Hours: Mon./Wed. 18:15 -- 19:00pm (after class)

News

Abstract

Internet security has become part of everyday life where security problems impact practical aspects of our lives. Even though there is a considerable corpus of knowledge about tools and techniques to protect systems, information about what are the actual vulnerabilities and how they are exploited is not generally available. This situation hampers the effectiveness of security research and practice. Understanding the details of attacks is a prerequisite for the design and implementation of secure systems.

This course deals with common programming, configuration, and design mistakes and ways to detect and avoid them. Examples are used to highlight general error classes, such as stack and heap overflows. Possible protection and detection techniques are examined. The course includes a number of practical lab assignments where participants are required to apply their knowledge as well as a discussion of the current research in the field. Students will learn how the security of systems can be violated, and how such attacks can be detected and prevented.

The course aims to make the students "security aware", and gain an in-depth understanding about security issues.

Tentative Syllabus

• Introduction & Principles
• Reconnaissance
• Unix Security Part
• Web Security Part
• Memory - Operational Semantics & Stack
• Memory - Assembly Primer
• Memory Corruption - Vulnerabilities
• Reverse Engineering
• Mobile Security
• Malware

With Topics On

• Operating system security and vulnerabilities (UNIX, Windows, stack and heap overflows)
• Windows Security
• Buffer Overflows (including Heap overflow)
• Testing
• Reverse engineering and binary analysis
• Viruses, worms, malware and malicious code
• Botnets
• Language security
• Web security
Prerequisites

Significant Programming experience (this course is not for you if you are a beginner)
Operating Systems knowledge (e.g., EC440)
Knowledge of C useful, C++ less useful
Basic SQL knowledge
Basic web programming knowledge

Dates and Times

Mondays 16:30 -- 18:15, PHO 203 & Wednesdays 16:30 -- 18:15, SCI 117

Practical Challenges (Homework Assignments)

Students will "need" to solve a set of practical challenges (assignments) in the lab part of the course. For more information on the challenges and the grading, check this page.

The current challenge is Challenge 4.

Grading

The course grade will be based on:

20%: Midterm exam
25%: Final exam
25%: 8 practical security challenges
25%: Security Project
5%: Participation

Registration

Registration details will be announced via e-mail to the registered participants.