SOFTWARE SECURITY

EECS 480H

COURSE DESCRIPTION: This course begins with discussions of good software engineering practices to ensure security in modern software systems and additional challenges to security due to code mobility in software for mobility-driven computing. The basics of software security and threat models, methods to protect software (operating systems, databases, distributed software)—including risk analysis, authentication and authorization, access control, and software architecture for security—are studied. Principles of secure coding, validation and verification of secure software, software and data watermarking, code obfuscation, tamper resistant software are studied, as well as the benefits of open source and closed source software. Use of software as an attack mechanism and emerging attack models (including joint hardware-software attacks) are studied. (3 credit hours)

FACULTY: To be announced


COURSE OBJECTIVES: This course is designed to provide a strong foundation in software security.

COURSE GRADE:

Exams (30%): 3 Exams, 1 every 3-4 weeks
Homework (40%): 4 assignment, ~ biweekly
Project (30%): Building on the homework to integrate and instill the learning experience.

WEEKLY COURSE SCHEDULE:
1. Introduction to software security; Hashing for Message Authentication
2. TCP/IP Vulnerabilities
3. DNS and the DNS Cache Poisoning Attack
4. Firewalls
5. PGP, IPSec, SSL/TLS, and Tor Protocols
6. The Buffer Overflow Attack
7. Malware: Viruses and Worms
8. Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing
9. Dictionary Attacks; Rainbow-Table Attacks
10. Security Issues in Structured Small-World Peer-to-Peer Networks
11. Web Security: PHP Exploits and the SQL Injection Attack; Cross-Site Scripting and Other Browser-Side Exploits
12. Bots and Botnets
13. Mounting Targeted Attacks with Trojans and Social Engineering—Cyber Espionage
14. Filtering Out Spam
15. Embedded Software Security Issues; Bus snooping Attacks and Embedded Software Infection

University Student Ethics Policy
http://studentaffairs.case.edu/ai/policy.html
Violations of the Student Ethics Policy will result in failure in the assignment in question or the course, or referral to the academic integrity board as per university policy.

All forms of academic dishonesty including cheating, plagiarism, misrepresentation, and obstruction are violations of academic integrity standards. Cheating includes copying from another’s work, falsifying problem solutions or laboratory reports, or using unauthorized sources, notes or computer programs. Plagiarism includes the presentation, without proper attribution, of another’s words or ideas from printed or electronic sources. It is also plagiarism to submit, without the instructor’s consent, an assignment in one class previously submitted in another. Misrepresentation includes forgery of official academic documents, the presentation of altered or falsified documents or testimony to a university office or official, taking an exam for another student, or lying about personal circumstances to postpone tests or assignments. Obstruction occurs when a student engages in unreasonable conduct that interferes with another's ability to conduct scholarly activity. Destroying a student’s computer file, stealing a student's notebook, and stealing a book on reserve in the library are examples of obstruction.