

CS 166: Introduction to Computer Systems Security

Sem. II, 2007–2008

Roberto Tamassia

This course teaches general principles of computer security from an applied viewpoint and focuses on providing hands-on experience in dealing with current security threats and available countermeasures. Students will learn about common cyber attacks (including viruses, worms, password crackers, keystroke-loggers, denial of service, spoofing, and phishing), tools for defending against such attacks, and methods for designing secure systems. In-class live demonstrations will be given.

Because of its minimal prerequisite, the course is targeted at sophomore and junior students. However, it can be taken also by more advanced undergraduate students and by graduate students. In addition to teaching computer security principles and the design of secure computer systems, the course also provides an overview of the fields of networking, operating systems, and cryptography.

Prerequisites The prerequisite for this course is either CS 16 or CS 18. No prior knowledge of computer security is assumed.

Topics The lectures and assignments will cover the following topics:

1. Introduction: overview of systems security, terminology, ethical issues
2. Operating Systems: basic concepts (users, processes, files, access control, authentication)
3. Malware: viruses, worms, spyware, rootkits, defenses
4. Broader Issues: social and legal aspects, social engineering
5. Networks: basic protocols (ARP, IP, TCP, UDP)
6. Networks: application-level protocols (DNS, HTTP, SMTP), firewalls
7. Networks: wireless networks
8. Symmetric Cryptography: block ciphers (DES, 3DES, AES), Kerberos
9. Public Key Cryptography: RSA, key exchange, pseudo-random number generators
10. Hash Functions: design (MD5, SHA), message authentication codes, hash trees
11. Data Security: encrypting file systems, Bitlocker, outsourced data
12. Digital Rights Management
13. Communication Security: SSH, TLS, stream authentication
14. System Administration
15. Broader Issues: economic aspects, human factors
16. Web Security: dynamic code, ActiveX, cross-site scripting
17. Web Security: cookies, SQL injection, single-signon
18. Physical Security: lockpicking, urban exploration
19. Digital cash, email security
20. Biometric authentication, RFID
21. Hardware Security: keylogging, eavesdropping RF emissions, smartcards, trusted platform modules

Labs In addition to the lectures, there will be five recommended tutorial sessions on the following subjects: internet lab setup, VMware, cracking tools, and Ethereal.

Reading Since computer systems security is an emerging field in rapid evolution, no existing textbook is suitable for this course. Detailed class notes and presentations prepared by the course staff will be provided, as well as an extensive list of articles and book excerpts.

Assignments and Grading The course assignments consist of four programming projects in Java (60% of the final grade) and five homeworks (40% of the final grade).

Programming Projects The programming projects consist of implementing portions of fundamental security applications, such as anti-virus tools, network firewalls, media players, and vulnerability testing systems. While students do not implement the entire application (a major task beyond the scope of the course), they are exposed to the design of such systems and they develop key components of them.

Sentinel: The goal of this project is to introduce students to the design of anti-virus software. They are introduced to a live compromised computer, asked to analyze excerpts of malicious code and discover its method of propagation and payload. Further, they implement a simulation program that assesses the threat posed by the discovered virus and extend an anti-virus system so that it will detect and clean-up a system infected by the virus.

SynCity: The goal of this project is to introduce students to networking firewalls and related tools. The students will create a port knocking daemon using iptables and pcap, and use this port knocking daemon to protect a service from outside attacks.

SecurePlayer: In this assignment, students will be presented with a rights management system for digital music. They will perform an analysis of the vulnerability of the system to various types of attacks aimed at bypassing the protection schemes, implement programs that demonstrate the identified vulnerabilities, and develop and test patches to the system to improve its security. The assignment will cover the basics of encryption protocols, both symmetric and asymmetric keys, as well as exchange protocols.

Wargames: This project is meant to test the cumulative knowledge of students of security vulnerabilities and test their skills in discovering potential weakness and securing real-life systems against attack. Students will be working in teams of two and will be provided with a machine that they would need to analyze and protect. Afterwards, as an experimental and fun class exercise, they will be able to practice “capture the flag” using as targets machines secured by their peers.