CSE 178: Computers and Networks Security (TR 6-7:15PM, in SSB 120)

Credits: 4
Instructor: Mukesh Singhal, *Professor*.
E-mail: msinghal@ucmerced.edu.
Office Hours: TR 9:30-10:30AM.
Office Location: SE2, Room 207.

Course Description

The following topics will be covered in roughly the given order.

1. Introduction: what is the problem?
2. Networking (levels, firewalls, sniffing)
3. Security models (military)
4. Encryption (types of attacks, uses of secret-key and public-key cryptography, uses of hash algorithms)
5. Algorithms (secret key: DES, IDEA, Rijndael, CBC, CFB, OFB, CFB; hashing: MD5, SHS; public-key: RSA, DSS)
6. Authentication (key distribution, passwords, addresses, cryptographic, certificates, nonces, Kerberos)
7. Pitfalls (security handshake attacks, performance problems)
8. Electronic mail (establishing keys, privacy, source authentication, message integrity, non-repudiation, PEM, PGP, X.400)
9. Public-key infrastructure (PKI)
10. Malware (viruses, worms, Trojan horses, service attacks, distributed denial-of-service, rootshell, repositories)
11. Legal, social and ethical issues (key escrow, export rules)

Prerequisites

Basic understanding of operating systems and computer networks, and basic knowledge of number theory, or consent of the instructor.

Examinations

There will be one in-class mid-term examination during the semester (Thursday, October 26, 2017) and a three-hour final examination (Wednesday, December 13, 2017, 11:30AM-2:30PM).

Grading

A student's grade will be determined by a weighted average of homework and lab. assignments, mid-term examination, and the final examination.

Homeworks or lab. assignments: 30%
Mid-term: 30%
Final Examination: 40%
Letter Grades: Letter Grades: A => 90, B => 80, C => 70.

Course Learning Outcomes

The students will demonstrate understanding of the following concepts in the design and development of secure computer networks: various security threats, security models, types of attacks, secret-key and public-key cryptography and algorithms, authentication methods, secure Electronic mail, Public-key infrastructure (PKI), various malware (viruses, worms, Trojan horses, etc.), distributed denial-of-service attacks, Firewalls, and legal, social and ethical issues (key escrow, export rules). Students will be able to analyze security threats in a system and design appropriate security measures for them. Students will be able to assess the performance overhead of using a security method and will be able to explain the price-performance and cost-security trade-offs of various methods.

Program Learning Outcomes

- Ability to design and conduct experiments and numerical simulations of complex electrical, electronic and computer systems, to analyze, and interpret general scientific and engineering information.
- A dedication to advance engineering research to discover new knowledge, develop new methodologies, promote innovative thinking and research output in engineering and science.

Academic Honesty

Students are expected to abide by the UC Merced campus-wide Academic Honesty Policy which can be found at http://studentlife.ucmerced.edu/what-we-do/student-judicial-affairs/academicy-honesty-policy. Academic misconduct is a serious offense. Violation of these policies may result in a grade of "F" or 0 points for the assignment or exam, or for more serious violations, a grade of "F" in the course, at the discretion of the instructor.

Special Needs

UC Merced provides individuals with disabilities reasonable accommodations to participate in educational programs, activities, and services. Students with disabilities requiring accommodations to meet course requirements should contact the UCM Disability Services Center (http://disability.ucmerced.edu/) to obtain assistance and coordination with this course.

Textbook

William Stallings
Cryptography and Network Security: Principles and Practices
Pearson-Prentice-Hall, 7th edition.
ISBN-13: 978-0134444284
ISBN-10: 0134444280

Papers from the literature