CSci 283/CSci 172 Computer Security - 3 credits - Vora

Fall 2010 schedule: Tues., 6:10 - 8:40 pm, Rome 352

Instructor: Poorvi Vora, Philips 714

Office Hours: Tues, Thurs: 12-2, 3-4 pm. unless canceled in class.

Grader: Amin Teymorian. Email: amin@gwu.edu

Course Website: http://www.seas.gwu.edu/~poorvi/Classes/CS283/

Purpose of course: To provide a broad overview of computer security at the advanced undergraduate/introductory graduate level.

Course content: Introductory cryptology and cryptographic protocols; program, database and network security; trusted operating systems; vulnerabilities/threats, attacks, defenses; administration of security; security policy.

Prerequisites: Undergrad level discrete math, programming, computer organization.

Text: *Computer Security: Art and Science* by Matt Bishop.

Grading: 30% for homework; 15% each for two in-semester tests; 15% for quizzes; 25% for final. All HWs will be submitted in Blackboard. **You will not be allowed the use of laptops, PDAs or calculators and similar devices during quizzes and in-semester tests**.

Undergraduate and graduate students will be graded separately. Graduate students will have extra assignments. *If you are an undergraduate and wish graduate credit for this class, contact your adviser. Graduate credit is NOT automatically obtained by undergraduates through registration for the graduate course.*

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the tests and quizzes. You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

Any violations will be treated as violations of the Code of Academic Integrity.

Any student who feels s/he may need an accommodation based on the impact of a disability should contact me privately to discuss specific needs. Please contact the Disability Support Services office at 202.994.8250 in the Marvin Center, Suite 242, to establish eligibility and to coordinate reasonable accommodations. For additional information please refer to: http://gwired.gwu.edu/dss/.

Syllabus: This is a tentative syllabus. There will be pop quizzes throughout the semester, most weeks.

Week I 31 August: Introduction. Classical Ciphers.
Chapters 1, 9.1, 9.2.1, 9.2.2, Text.

Week II 7 September: Stream and Block Ciphers and Public Key Cryptography.
Chapters 9.2.3, 11.2, 9.3, 9.4, Text.

Week III 14 September: Public Key Infrastructure.
Chapter 10, except 10.2.2, 10.3 and 10.5, Text.

Week IV 21 September: Access Control.
Chapters 2 and 15 (part of), Text.

Week V 28 September: Access Control, contd.
Chapters 2 and 15 (part of), Text.

Week VI 5 October: Test 1.

Week VII 12 October: Birthday and replay attacks. Schneier Attack Trees. Security Policies.
Chapter 4 (except 4.5 and 4.6), Text.

Week VIII 19 October: Confidentiality, Integrity and Hybrid Models.
Chapters 5.1, 5.2.1, 6.1, 6.2, 7.1, 7.2 from text

Week IX 26 October: Authentication, Confinement. Design Principles.
Chapters 12, 13, 17. Text.

Week X 2 November: Trusted OS

Week XI 9 November: Test 2

Week XII 16 November: Identity, Covert Channels and Malicious Logic.

Week XIII 23 November: Privacy and Risk Analysis

Week XIV 30 November: Voting