

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

Fall 2005 schedule: Tues., 7:10 - 9:40 pm, Gelman 607

Instructor: Poorvi Vora, Philips 706

Office Hours: 2-5 pm Tues. unless cancelled in class. Also by appointment through email.

TA: Yu-An Sun. Email: ysun@gwu.edu Office Hours: 12:30-2 and 5-6:30, Tuesdays and 4-7 pm, Thursdays.

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: Discrete math, introductory programming, computer organization; all at the undergraduate level.

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

Grading: 30% for homework, 35% for in-semester test, 35% for final. Grading will be absolute and not on a curve. All HWs will be submitted in Blackboard.

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 test and final.

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.

Syllabus: This is a tentative syllabus.

Week I 6 September: Introduction and Access Control. Chapters 1, 2 and 15 (part of), Text.

Week II 13 September: Foundational Results (Take-Grant Protection Model). Chapters 15 and 3 (part of), Text. HW1 assigned.

Week III 20 September: Security Policies. Confidentiality and Integrity. Chapters 4, 5 and 6, Text. HW1 due. HW2 assigned.

Week IV 27 September: Hybrid Policies. Classical and Symmetric-Key Ciphers. Chapters 7 and 9 (part of). Text.

Week V 4 October: Public Key Cryptography. Key management. Chapters 9 and 10. Text. HW2 due. HW3 assigned.

Week VI 11 October: Cipher Techniques. Chapter 11, Text. HW3 due.

Week VII 18 October: Test. Material Covered in Lectures I-VI.

Week VIII 25 October: Return Test. Discuss. Authentication and Identity. Chapters 12 and 14 (part of), Text. HW4 assigned.

Week IX 1 November: Identity. Design Principles, Information Flow. Chapters 14, 13, 16. Text.

Week X 8 November: Confinement. Introduction to Assurance, Formal Methods. Chapters 17, 18, 20. HW4 due. HW5 assigned.

Week XI 15 November: Systems with Assurance, Evaluating Systems. Chapter 19 and 21, Text. HW5 due. HW6 assigned.

Week XII 22 November: Malicious Logic. Chapter 22, Text. Begin Trusted OS. HW6 due.

Week XIII 29 November: Complete Trusted OS. Database Security.

Week XIV 6 December: Final. Material Covered in Lectures VIII-XIII.