Wright State University

CORE Scholar

Winter 2011

CS 790-01: Information Security

Meilin Liu
Wright State University - Main Campus, meilin.liu@wright.edu

Repository Citation

Computer Science (CS) 790
Information Security

Winter Quarter 2011
Wright State University

Course Description

This course gives a comprehensive study of security vulnerabilities in information systems and the basic techniques for developing secure applications and practicing safe computing. Topics include: Conventional encryption; Data Encryption Standard; Advanced Encryption Standard; Hashing functions and data integrity; Basic Number Theory; Public-key encryption (RSA); Digital signature; Security standards and applications; Access Control; Management and analysis of security. After taking this course, students will have the knowledge of several well-known security standards and their applications; and the students should be able to increase system security and develop secure applications.

Lecturer
Meilin Liu
Office: 353 Russ Engineering Center
Phone: 937-775-5061
Office Hours: Monday/Wednesday 3:00 – 5:00 pm
Email: meilin.liu@wright.edu
Web: www.wright.edu/~meilin.liu

Class
* Monday/Wednesday 6:05 - 7:20 pm MC RC 406

Text
Cryptography and Network Security, Third Edition or Fourth Edition, by William Stallings, Prentice Hall.

Reference
Matt Bishop, Computer Security: Art and Science, Addison Wesley, 2003.
Charles Pfleeger and Shari Pfleeger, Security in Computing, Third Edition, Prentice Hall, 2003.

Prerequisite: Computer Organization (CEG 320), and Data Structures and Algorithm (CS 400) or with the permission of the instructor

Required Work (Subject to change)

Homework	20%	(5 homeworks)
Quizzes	10%	(4 quizzes)
Project	25%	(1 to 2 projects)
Midterm	20%	
Final Exam	25%	

Grading

The base scale is: A: 90-100, B: 80-89, C: 70-79, D: 60-69, F: 0-59. This is the highest requirement that will be used. The scales may be lowered or revised if necessary.

Schedule

(The schedule may subject to change.)

Week	Contents	Reading
1	Overview of Security; Common Security Attacks	Chap1
2	Conventional Cryptography	Chap2
3	Block Ciphers and DES	Chap3
4	Introduction to Number Theory	Chap8
5	Public Key cryptography and RSA	Chap9
6	Diffie-Hellman Key Exchange System; Introduction to Finite Fields	Chap10;chap4
7	Advanced Encryption Standard	Chap5
8	Hash Functions & Secure Hash Algorithm	Chap11; Chap12
9	Data Integrity & Digital Signature	Chap13
10	Access Control; Security Models	From reference books
	Final Exam: March 16th, 2011, 8:00-10:00pm	

Policies and Notes

- Attendance: Attendance is not required, but class participation is important. For your own sake, you should not miss any of the classes. If you are not a regular attendee, it will be your responsibility to seek out what material was covered in the lecture and learn it. Most of my exam questions will be taken directly from ideas covered during the lecture, so it greatly helps if you attend!

- I will utilize webCT (wisdom.wright.edu) to post updates to the course, solutions, assignments, announcements, schedule, etc. Get in the habit of checking it regularly.

- If you are going to miss an exam, for any reason, discuss it with me in advance. If it is an emergency situation, please notify me as soon as possible.

- A penalty of 10% deduction each day for late submission of homework will be given and after 5 days, 0 point will be given.

- If you need to meet me other than my office hours, better make an appointment by email or by phone beforehand.

Academic Misconduct

In this class, the only way to truly learn the concepts to is do the work yourself. I encourage working with other people on the course concepts. When you begin to do the homework and the projects, do it on your own.