

Wright State University

CORE Scholar

Computer Science & Engineering Syllabi

College of Engineering & Computer Science

Fall 2008

CS 790: Information Security

Meilin Liu

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

Follow this and additional works at: https://corescholar.libraries.wright.edu/cecs_syllabi



Part of the [Computer Engineering Commons](#), and the [Computer Sciences Commons](#)

Repository Citation

Liu, M. (2008). CS 790: Information Security. .
https://corescholar.libraries.wright.edu/cecs_syllabi/226

This Syllabus is brought to you for free and open access by the College of Engineering & Computer Science at CORE Scholar. It has been accepted for inclusion in Computer Science & Engineering Syllabi by an authorized administrator of CORE Scholar. For more information, please contact library-corescholar@wright.edu.

Computer Science (CS) 790

Information Security

Fall Quarter 2008
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; Hashing functions and data integrity; Public-key encryption (RSA, Elliptic-Curve); Digital signature; Block cipher; Watermarking for multimedia; Security standards and applications; Building secure software and systems; Management and analysis of security; Legal and ethical issues in computer security.

Lecturer

Meilin Liu

Office: 353 Russ Engineering Center

Phone: 937-775-5061

Office Hours: Monday/Wednesday 2:00 – 4:00 pm

Email: meilin.liu@wright.edu

Web: www.wright.edu/~meilin.liu

Class

- Monday/Wednesday 8:00 – 9:15 Russ 155

Prerequisite: Digital System and Operating System or with the permission of the instructor

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.

Required Work (Subject to change)

Homework	20%
Quizzes	10%
Project	30%
Midterm	20%
Final Exam	20%

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.

Topics:

Overview of Security
Information Security Basics
Common Security Attacks
Conventional Cryptography
 Classical Encryption Techniques
 Block Ciphers and DES
 Introduction to Finite Fields
 Advanced Encryption Standard
Public-Key Encryption
 Introduction to Number Theory
 RSA cryptography
 Key Management & Other Cryptosystems
Hash Functions & Data Integrity
Digital Signature
Security Practice in Email, Web
Security in OS

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.
- Always make back ups of all of you work. Never have just one copy of anything!
- 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.