Fall 2012

CS 7900: 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**  
https://corescholar.libraries.wright.edu/cecs_syllabi/307

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.
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 2:00 – 4:00 pm
Email: meilin.liu@wright.edu
Web: www.wright.edu/~meilin.liu

Class
- Monday/Wednesday 07:40 pm - 09:00pm MC RC 302

Text

Reference

Prerequisite: Computer Organization (CEG 3310), and Data Structures and Algorithm (CS 3100) or with the permission of the instructor

Required Work (Subject to change)
Homework 20% (5 to 6 homeworks)
Quizzes 10% (4-5 quizzes)
Project 25% (2 to 3 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.)

<table>
<thead>
<tr>
<th>Week</th>
<th>Contents</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview of Security; Common Security Attacks</td>
<td>Chap1</td>
</tr>
<tr>
<td>2</td>
<td>Conventional Cryptography</td>
<td>Chap2</td>
</tr>
<tr>
<td>3</td>
<td>Block Ciphers and DES</td>
<td>Chap3</td>
</tr>
<tr>
<td>4</td>
<td>Introduction to Number Theory</td>
<td>Chap8;chap4</td>
</tr>
<tr>
<td>5</td>
<td>Public Key cryptography and RSA</td>
<td>Chap9</td>
</tr>
<tr>
<td>6</td>
<td>Diffie-Hellman Key Exchange System; Introduction to Finite Fields</td>
<td>Chap10;chap4</td>
</tr>
<tr>
<td>7</td>
<td>Advanced Encryption Standard</td>
<td>Chap5</td>
</tr>
<tr>
<td>8</td>
<td>Hash Functions &amp; Secure Hash Algorithm</td>
<td>Chap11; Chap12</td>
</tr>
<tr>
<td>9</td>
<td>Data Integrity &amp; Digital Signature</td>
<td>Chap13</td>
</tr>
<tr>
<td>10</td>
<td>Access Control; Security Models</td>
<td>From reference books</td>
</tr>
<tr>
<td>11</td>
<td>User Authentication</td>
<td>From reference books</td>
</tr>
<tr>
<td>12</td>
<td>Intrusion Detection</td>
<td>Chap20</td>
</tr>
<tr>
<td>13</td>
<td>Intrusion Detection</td>
<td>Chap20</td>
</tr>
<tr>
<td>14</td>
<td>Elliptic Curve Cryptography</td>
<td>Chap10</td>
</tr>
<tr>
<td>15</td>
<td>Legal and Ethical Issues in Security</td>
<td>Chap 23</td>
</tr>
<tr>
<td></td>
<td>Final Exam: December 12, 2012 (Wednesday), 8:00-10:00pm</td>
<td></td>
</tr>
</tbody>
</table>

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! Pop up quizzes will be given. If you miss a class, you might also miss a pop up quiz.
- I will utilize Pilot (pilot.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.