CPE 645 Computer Network Security

Fall 2011, TTh 12:45-2:05 p.m. EB 240

Course Objectives:

This course covers network security technology, the latest standards for security in the Internet working environment, and the practical issues involved in developing security applications. The main contents are introduction to cryptography, confidentiality, authentication, digital signatures, e-mail security, IP security, web security, and other network security-related issues.

Required Textbook:

Cryptography and Network Security: Principles and Practice, 5th edition, by William Stallings, Prentice Hall, ISBN: 0-13-187316-4

Reference Papers: TBA

Course Prerequisites:

CPE 448/548 Introduction to Computer Networks or equivalent

Instructor:

Dr. Seong-Moo (Sam) Yoo
Office: EB 217-D, **Phone:** (256) 824-6858, **Email:** yoos@eng.uah.edu
Office Hours: TTR 2:15-3:30 p.m., and by appointment

Course Web Page:

- Angel course management software will be used to assist in course administration. Students may access Angel via the URL listed below.

  http://angel.uah.edu

- Each student is responsible for checking the course Angel page for assignment updates and due dates, and other course related announcements.

Course Grade Computation:

Homework: 25%
Project: 20%
Exam 1: 20%
Exam 2: 30%
Class participation and presentation: 5%

Total 100%

- Students may track their progress by examining their grades on Angel.

- Exam/homework/project grade discrepancies must be reported to the instructor no later than two weeks once the grade has been posted online.

Attendance Policy:

All students are expected to attend all course lectures. Angel will be used to ***assist*** in course administration. This course, however, is **not** an "online course". I do check your attendance randomly, not every day.

Academic Honesty:

- Collaboration on exam/quiz will not be permitted and will be considered cheating.

- Students who cheat will receive **no credit (0)** for that test/exam or project and be reported to the University Judicial Officer.

Plagiarism Policy:

Free exchange of ideas is fine. However, the transfer of ideas into written or machine format is strongly prohibited. It is the sole responsibility of the student submitting the work for grading. Therefore, students are not to take credit for the idea or written work of someone else. All parties collaborating in the plagiarism process are equally liable.

Student with disabilities:

The instructor would like to hear from anyone who has a disability that may require a modification of seating, testing, or other class procedures. Please see the instructor after class or during office hours to discuss appropriate modifications. You should also contact Student Development Services in UC 113 (Ph. 824-6203) for further assistance.

Exam Policies:

Exam questions may be drawn from information presented during the class lectures or material from the assigned textbook readings.

Noise Policy:

- If your Cell Phone, Pager, or PDA rings during a test/exam, the instructor will take your exam and will grade it as it is. You will not be allowed to complete your exam, and you will not be allowed to take a makeup exam.

- If your Cell Phone, Pager, or PDA rings during lecture, the instructor may elect to leave the room. In this case, students will be responsible for learning on their own the material that would have been presented during that lecture.

Project Policies: TBA

Disclaimer:

The instructor reserves the right to amend this syllabus as needed.
Any updates to the syllabus will be posted on the course Angel page.

Course Outline:

Overview

1. Mathematical Background
   Introduction to finite fields
   Introduction to number theory
   Introduction to elliptic curve arithmetic
2. Cryptography
   Block ciphers and Data Encryption Standard (DES)
   Advanced Encryption Standard (AES)
   Diffie-Helman, RSA, Al-Gamal
   Elliptic curve cryptography
   Quantum cryptography
3. Security service
   Confidentiality
   Message authentication and hash functions
   Digital signatures and authentication protocols
4. Network security
   Authentication applications
   E-mail security
   IP security
   Web security
5. Other issues
   5.1 Intrusion detection
   5.2 Computer worm
   5.3 Wireless network security
   5.4 Others

Tentative course schedule

- Make sure that this is a tentative schedule. This schedule can be changed. Check announcements in class.

Week	Date	Covered material	Remark
1	8/18	Overview of crypto	
2	8/23	Classical encryption and S-DES	
	8/25	DES	
3	8/30	DES, Finite Field	
	9/1	Finite Field	
4	9/6	AES	
	9/8	AES, Triple-DES	
5	9/13	Block cipher mode	
	9/15	Confidentiality using symmetric encryptions	
6	9/20	Number theory	
	9/22	Number theory, project proposal presentation	
7	9/27	Exam 1 preview, project proposal presentation	
	9/29	Exam 1	9/29 Exam 1
8	10/4	RSA	
	10/6	No class	10/6-10/7 Fall break

9	10/11	Key management, Deffie-Helman, Al-Gamal	
	10/13	Elliptic curve arithmetic	
10	10/18	Elliptic curve arithmetic	
	10/20	Elliptic curve cryptography, message authentication	
11	10/25	Hash functions, MD5	
	10/27	Secure hash algorithms (SHA)	
12	11/1	Digital signatures	
	11/3	E-mail security, IP security	
13	11/8	IP security, web security	
	11/10	Quantum crypto	
14	11/15	Intrusion detection and computer worm	
	11/17	Wireless network security	
15	11/22	Student presentations	
	11/25	No class	11/24-11/25 Thanksgiving holiday
16	11/29	Student presentations	11/29 last class
17	12/6	Final exam 11:30-2:00 p	