CSCI 420/520: Computer and Network Security
Spring 2006

Basic Information
Time & Place: MW 4:30-5:50, James Blair Hall #223
Th 2:00-3:20, as needed for make-up lectures
Instructor: Haining Wang, 141 McGlothlin-street Hall, Email: hnw@cs.wm.edu
Office Hours: TR 2:00-4:00pm, or by appointment
Teaching assistant: Chuan Yue, 107 (B) McGlothlin-street Hall, Email: cyue@cs.wm.edu
Office Hours: MW 3:30-5:00am,
Course web page: http://www.cs.wm.edu/~hnw/courses/cs420/cs420.html

Course Overview
This is an upper-level undergraduate, first-year graduate course on network and computer security. This course introduces the principles and practices of cryptography and network security. The first half of the class content covers basic cryptographic methods, key distribution, and protocols for authenticated and confidential communications. Topics include block and stream ciphers, confidentiality, traffic analysis, key distribution, random number generation, public key cryptography, RSA, Needham-Schroeder protocol, Diffie-Hellman key exchange, one-way hash functions, message authentication codes, birthday attack, MD5, SHA-1, HMAC, digital signatures, mutual authentication, and replay attacks.

The latter half of the class content addresses the practice of network security. Topics include Kerberos, PGP, public key infrastructures, SSL/TLS, IP security, intrusion detection, password management, firewall, virus and worms, and Denial of Service (DoS) attacks. The lecture will be conducted in an interactive fashion. A group of two or three students will identify and work on a research project. Plus, there will be about five homework assignments, and midterm and final exams

Course Prerequisites

- Familiarity with basic networking protocols.

Grading Policy
Grades will be computed as follows:
15% Homeworks
25% Term Project
25% Mid-term Exam
35% Final Exam

Required textbooks (available at online bookstores)

William Stallings
Prentice Hall Publishing.

Supplementary textbooks

Ross Anderson
Wiley Computer Publishing
Lecture schedule (tentative)
The following lists our lecture schedule. This schedule is subject to change as the course develops; changes will be announced in class.

1st Week
Introduction and Overview
Read: Chapter 1

2nd Week
Classical Encryption Techniques
Read: Chapter 2.1, 2.2, 2.3, and 2.5

3rd Week
Block Cipher (DES and AES)
Read: Chapter 3.1, 3.2, 3.3, 3.4, 3.6, 3.7 (3rd edition); 3.1, 3.2, 3.3, 3.5 (4th edition); and Chapter 5.1, 5.2

4th Week
Triple DES, Blowfish, RC5 and Stream Cipher RC4
Read: Chapter 6.1, 6.2, 6.3, 6.4 and 6.5

5th Week
Placement, Traffic Confidentiality, Key distribution and RNG
Read: Chapter 7.1, 7.2, 7.3 and 7.4

6th Week
Public-key Encryption
Read: Chapter 9.1, 9.2, 10.1, and 10.2

7th Week
Message Authentication and Hash Function
Read: Chapter 11.1, 11.2, 11.3, 11.4, 11.5, 12.1, 12.2, 12.3

8th Week (Spring Break)

9th Week
Digital Signatures
Read: Chapter 13.1 and 13.2

10th Week
Kerberos and PGP
Read: Chapter 14.1, 14.2 and 15.1

11th Week
IP Security
Read: Chapter 16.1 – 16.6

12th Week
Web Security
Read: Chapter 17.1 and 17.2

13th Week
Intrusion Detection and Firewall
Read: Chapter 18.1, 18.2, 18.3 and 20.1