CSCI 454/554: Computer and Network Security
Spring 2008

Basic Information
Time & Place: TR 3:30-4:50, M-S Hall #020
M 2:00-3:20, as needed for make-up lectures
Instructor: Haining Wang, 105 McGlothlin-street Hall, Email: hnw@cs.wm.edu
Office Hours: TR 1:00-3:00pm, or by appointment
Teaching assistant: Sean Krems, 107 (C) McGlothlin-street Hall, Email: smkrem@cs.wm.edu
Office Hours: T 9:30am-11:00am, W 4:30-6:00pm
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 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)

Cryptography and Network Security: Principles and Practice, Third or Fourth Edition
William Stallings
Prentice Hall Publishing.

Supplementary textbooks

Ross Anderson
Wiley Computer Publishing