

MSI 604 (Call # 4685)
Communications, Networking and Computer Security
University at Albany, SUNY
Spring 2004

Instructor Information

Name: Sanjay Goel / Jakov (Yasha) Crnkovic
Email: goel@albany.edu / yasha@albany.edu
Phone: (518) 442-4925 / (518) 442-5318
Office Hours: (Goel) M 1:00-2:30 or by appointment / (Yasha) M 10-11:30 & TH 1-2
Office Location: BA 310b / BA 332

Class Information

Time: 9:05-12:10
Room: BA233
Dates: September - December
Available Labs: MIS/HRIS/Security Lab

Course Overview

This course covers Data Communications, Computer Networking and Computer Security. The first module of the course focuses on communications where we discuss fundamentals of signal transmission, transmission hardware and basic communication concepts such as error control and multiplexing. The second module of the class covers Network Topologies, the OSI model, and the TCP/IP protocol suite. This module also covers the various architectures used on the Internet, including client-server, peer-to-peer and n-tier architectures. Also covered is network switching and schemes for routing data on the network. Students will have the opportunity to use network simulation tools. In the third module of the class, vulnerabilities of computer networks and techniques for protecting networks and data are discussed. Basic elements of symmetric and asymmetric cryptography are discussed. Secure Electronic Commerce, involving secure transmission, authentication, digital signatures, digital certificates and Public Key Infrastructure is also presented. Issues in privacy, ethics and policies are also discussed where students study technologies like Web Bugs and Carnivore and debate on ethical issues related to privacy.

Learning Objectives

- Students learn the basic concepts of Communications & Computer Networks
- Students learn to use simulation tools for designing & optimizing communication network topologies
- Students understand the basic concepts of cryptography and Public Key Infrastructure
- Students learn to analyze security threats to computer networks and the means to protect them
- Students learn to research in the focused area of Networks & Security
- Students develop critical thinking skills via debates on the ethics and legal issues involved in electronic data access.

Immersion Classes

The class is usually supplemented by 2-3 immersion classes which are full day classes covering special topics in Computer security. The content of the classes may vary based on the interest of the audience and the availability of the instructor. This is not a mandatory part of the class and is strictly volunteer (without any grade implication) based on the interests of the students. The three potential classes are:

Security Programming using Java - In this class the students learn the basic cryptography classes in java and learn encryption and decryption of data. The students also learn to create message hashes, digital signatures and certificate servers.

Hacking Lab - In this lab students learn to use some hacking tools hands-on. These include password analyzers, network and port scanners and tools for denial-of-service attack as well as spoofing. The purpose of the lab is to train the students in better understand computer security issues in the organizations.

Distributed Computing using Jini - The class will be involved in the development of a service based architecture using Jini. Each student will develop a different service and the class will call each others services. The goal of the class is to teach the students the working and development of a peer-to-peer

system. As a part of the class the students will learn how to install, configure and deploy a peer-to-peer system

Books & Software

Text Book: Data Communications & Computer Networks: A Business Users's Approach by Curt M. White

Text Book: Security In Computing (Third Edition) by Charles P. Pfleeger & Shari Lawrence Pfleeger

Reference: Hackers Beware by Eric Cole

Reference: Professional Java Security by Jess Garms and Daniel Somerfield

Grading

Homework & Assignments: 50%

Exams: 50%

Term Paper (on Computer Security)

If either of the instructors assigns a term paper to the students they should make two person teams. Each team must complete a term paper from among the topics listed by the instructor. The paper should include a broad introduction of the topic and a comprehensive discussion of a few selected aspects of the topic. The paper will be presented. All students must be present for all the presentations. The students will be graded on the term paper as well as the quality of the presentations. The paper should not be four pages (single spaced, 12 pt text) long so the students should make an effort to write four pages of original text. The paper should reflect a clear understanding of the subject by the student. The presentation should not exceed more than five viewgraphs. Please use your critical thinking skills to be concise and focused on both the paper as well as the presentations.

An alternate scenario would be that the instructor would provide specific readings on different topics and would want the students to analyze the papers, critique them and present the analysis in the class. One of the two approaches will be picked in collaboration with the class.

Assignments

An assignment given in any week is due at the beginning of the class on the same day in the following week. There will be a penalty for late assignments unless there is a very pressing reason for the delay. Please work individually on all assignments. Stop by the instructor offices if you have difficulty in understanding the assignment or the course material discussed in the class.

Course Schedule

| Week | Date | Topics | Readings | Instructor |
|------|------|---|----------|------------|
| 1 | 1/22 | Introduction to Computer Networks and Data Communication; | 1,2 | Crnkovic |
| | | Fundamentals of Data and Signals; The Media | 3 | |
| 2 | 1/29 | Making Connections. Multiplexing. | 4,5 | |
| | | Errors, Error Detection And Error Control | 6 | |
| 3 | 2/5 | Local Area Networks | 7,8,9 | |
| | | WAN | 10 | |
| 4 | 2/12 | Exam I | | |
| | | Network Design and Management | 14 | |
| 5 | 2/19 | Network Design and Management (cont.). | 14 | |
| | | Telecommunication Systems; Implementation in various businesses | 12 | |

| | | | | |
|----|------|---|--|------|
| 6 | 2/26 | Introduction to Internet; OSI Model | | Goel |
| | | Network Architectures | | |
| 7 | 3/4 | Routing | | |
| | | Routing contd. | | |
| 8 | 3/11 | Introduction to Security | | |
| | | Hacker Attacks | | |
| 9 | 3/18 | Hacker Attacks | | |
| | | Watermarking and Steganography | | |
| 10 | 3/25 | Computer Forensics / Hacking Lab | | |
| 11 | 4/1 | Cryptography - Symmetric & Asymmetric | | |
| | | Public Key Infrastructure, Digital Signatures, Digital Certificates | | |
| 12 | 4/15 | Current Topics | | |
| | | Analyzing Computer Security Risk | | |
| 13 | 4/22 | Security Policy | | |
| | | Managing Computer Security Risk | | |
| 14 | 4/29 | Exam II | | |
| | | Ethics and Legal Issues | | |