ITM 604: Data Communications, Networks, and Security
University at Albany, State University of New York
Spring 2006 Syllabus

Instructor Information
Name: Sanjay Goel / Yasha Crnkovic
Email: goel@albany.edu / yasha@albany.edu
Phone: (Goel) 442-4925 / (Crnkovic) 442-5318
Office Location: (Goel) BA310b /(Crnkovic) BA332
Office Hours: (Goel) M 12:30pm - 2:00pm / MW 10-11:30am (Crnkovic) also by appointment

Class Information
Time: Thursdays 9:05am - 12:10pm
Location: BA 233
Dates: January 26 - May 4
Credit(s): 3   Call #: 4044   Available Lab(s): HRIS and MIS Labs

WebCT (Crnkovic): http://webct.albany.edu:8900
Website (Goel): http://www.albany.edu/~goel/classes/spring2006/itm604
These course websites should be your main sources of course material and contain all relevant course information including details on grading, projects, assignments, course schedule, etc. In addition, these should provide a "living syllabus" and will reflect any changes made to this document.

Text & Reference Books
Text (Crnkovic)- Data Communications & Computer Networks: A Business Users's Approach, Third Edition by Curt M. White, ISBN: 0619160357
Text (Goel)- Secrets and Lies: Digital Security in a Networked World (paperback) by Bruce Schneier, ISBN: 0471453803

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. Different wired and wireless media, such as, fiber optic, coaxial cables, cell phones, satellite microwave are also presented. Students learn the pros and cons of selecting different media types. 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 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. Students go through the process of information security risk analysis through a case study, which consolidates their learning in the modules and hones their critical thinking and analytic skills.

Learning Objectives

Students will learn:
1. Basic concepts of communications & computer networks
2. How to use simulation tools for designing & optimizing communication network topologies
3. Basic concepts of cryptography and Public Key Infrastructure
4. How to analyze security threats to computer networks and how to protect them
5. How to research in the focused area of computer networks & network security
6. Critical thinking skills via debates on the ethics and legal issues involved in electronic data access

Grading

All students are expected to follow University at Albany guidelines on academic integrity (see the Academic Integrity section for more detail). If any assignment or project submission contains any material (text, diagrams, code, etc.) generated by others (not on your project team), your submission must clearly indicate the source of such material. Failure to indicate the source of the material will be treated as plagiarism. Individuals must work on their own on assignments unless otherwise specified by the professor.

ASSIGNMENTS AND PROJECTS FOR PROF. GOEL'S PART

Assignments- 15%
Assignments can be in-class or take-home and will be designated as individual or group assignments depending on the specific assignments. Please see the Assignments section of the course site for further details and guidelines.

Project - 25%
The project will involve performing a risk analysis based on a case or on an organization that students have access to using the risk analysis methodology presented in class. Students will be provided an Excel spreadsheet in which to fill in the matrices for Assets/Vulnerabilities, Vulnerabilities/Threats, and Threats/Controls. Students also provide a written document in which they detail their reasoning for choosing specific values similar to that shown in the case example.

Paper 20%
The paper should be done in pairs or individually and no more than two people in a team and will focus on a security-related topic. If you work in groups of two, make sure that the work is equally divided. The point writing a paper is so that you learn how to do in-depth research on a topic, think carefully and deeply about the issues, and express your own ideas as clearly as possible. Suggested research topics will be provided and students will be given separate topics. Please see the Projects/Papers section of the course site for further details and guidelines.

ASSIGNMENTS AND PROJECTS FOR PROF. CRNKOVIC'S PART

The grade for the first part (= 1/3 of the final grade) will reflect the same ratio (60% assignments and 40% exam). There are 9 short projects from the first part of the course to be assigned to groups (groups are randomly generated on the WebCT and *please* do not ask for any changes since the first three projects are due for presentations in two weeks, 30%). Group 1 will solve the project 1, etc. Each group will prepare one project and submit their documents in appropriate group folder. In addition, each student will prepare one homework assignment (due after the President's week break, on March 16th) and upload it in the Assignment folder of the WebCT (30%). Exam is 40% see below.

Exam- 40%
There will be two exams in the class. The first exam will be multiple-choice and is open-book. It will cover what is learned during the first third of the class with Professor Crnkovic. The second exam will consist of multiple sections (essay-style) in which will cover networking and security. The will have to apply a majority of what has been learned during the last two-thirds of the semester in order to assess individual performance. This can include encryption, digital signature creation, and other topics discussed in the last two-thirds of the course. Students may use the recommended texts, class notes, and PowerPoint presentations. No use of electronic devices (laptops, cellphones, PDA's, etc.) is allowed during testing. A previous exam and sample solution set will be provided for review.

Course Schedule

Date	Topics	Readings	Assignments	Instructor
1/26	Introduction to Computer Networks and Data Communication	White 1 & 2	See WebCT	Crnkovic
	Fundamentals of Data and Signals; The Media; Making Connections	White 3 & 4		
2/2	Multiplexing; Errors, Error Detection and Error Control	White 5 & 6	See WebCT	
	Local Area Networks	White 7		
2/9	Local Area Networks, cont'd.	White 8 & 9	See WebCT	
	WAN; First three group presentations	White 10		
2/16	Network Design and Management; Six group presentations	White 14	See WebCT	
	Exam 1 (from 10:30am)	White 1-10		
3/2	Introduction to Internet; OSI Model	Lecture Notes		Goel
	Network Architectures	Lecture Notes		
3/9	Security Fundamentals	Schneier 1-5, 8 & 25	Paper Topics Assigned	
	Hacker Attacks	Schneier 9-12		
3/16	Hacker Attacks	Schneier 13, 14, 17 & 22		
	Analyzing Computer Security Risk	Schneier 18, 19 & 21		
3/23	Managing Computer Security Risk	Schneier 23 & 24	Paper Due Project Assigned	
	Computer Security Risk (Case Analysis)			
3/30	Security Policies	Schneier 20		
4/6	Security Policies Cont'd.	Schneier 20		
4/20	Computer Forensics / Hacking Lab	Class Handouts		
4/27	Cryptography, PKI, Digital Signatures & Certificates	Schneier 6, 7 & 15	Project Due	
5/4	Exam 2	Notes & Book		
	Watermarking/Steganography Lab	Schneier 16		