ITM 604: Data Communications, Networks, and Security
University at Albany, State University of New York
Spring 2008 - Syllabus

Instructor Information

Name: Sanjay Goel Email: goel@albany.edu Phone: 442-4925 Office Location: BA310b Office Hours: M 11:30pm - 1:00pm or by appointment	Name: Peter Duchessi Email: p.duchessi@albany.edu Phone: 442-4945 Office Location: BA312 Office Hours: TBD

Class Information

Time: Thursday 8:30 am – 11:30pm
Location: BA 233
Dates: January 24 - May 1
Credit(s): 3
Call #: 3813
Available Lab(s): HRIS and MIS Labs

Text & Reference Books

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

Course Overview

The class covers communications networking and security. Communications and networks drive business and industry and have helped in achieving unforeseen efficiencies. There has been a tremendous growth in related careers in these fields. This class is a capstone class that builds on your previous knowledge from the Business School and provides you with the skills that you need to enter into these fields.

In the first part of the class, you will cover different media types including: fiber optics, twisted pair, and co-axial cables. You will also get an understanding of mobile communication devices including cell phones, satellites, and other handheld devices. In addition, how data is modulated as it goes through different media will be covered.

In the second part of the class, we will discuss network topologies, the OSI/Internet models, and the TCP/IP protocol suite. This module also covers the various architectures used on the Internet, including client-server, P2P, 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, secure e-commerce, involving secure transmission, authentication, digital signatures, digital certificates and Public Key Infrastructure (PKI) is presented. Issues in privacy, ethics and policies are also discussed where students study and debate controversial topics such as government monitoring technologies. 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. Basic concepts of cryptography and Public Key Infrastructure
3. How to analyze security threats to computer networks and how to protect them
4. How to research in the focused area of computer networks & network security
5. Critical thinking skills via debates on the ethics and legal issues related to information technology

ASSESSMENT & 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 cite the source of such material. Failure to cite source material appropriately will be treated as plagiarism. Individuals must work on their own on assignments unless otherwise specified by the professor.

Assignments & Project Quizzes (30%)

Assignments can be in-class or take-home and will be designated as individual or group assignments depending on the specific assignment. Please see the Assignments section of the course site for further details and guidelines. An example of a project is to perform a risk analysis based on a case or on in organization using the risk analysis methodology presented in the class. For each class there will be a quiz either at the end of the class or the beginning of the next class that will test your learning in each class and class project.

Paper - 10%

The paper should be done in pairs and will focus on a security-related topic. Please make sure that the work is equally divided among the team members. Along with the submission, also list the contributions of each team member. The point of writing a paper is so that you learn to do in-depth research on a topic, think carefully and deeply about the issues, and express your own ideas as clearly as possible. Groups of students will discuss potential topics with the professor on the first day to determine a final paper topic. Please make sure that you see the Projects/Papers section of the course site for further details and guidelines prior to starting on your paper.

Exam I (Duchessi) - 30%: This exam will be an objective type exam that will cover the first third of the class.

Exam II (Goel) – 30%: This exam will consist of multiple sections (essay-style) which will cover the last 2/3 of the class.

Notes:

1. Students may use the recommended texts, class notes, and PowerPoint presentations for exams unless otherwise specified. No use of electronic devices (laptops, cellphones, PDA's, etc.) is allowed during testing.
2. Students who do not show up to take an exam and do not have a verifiable legitimate excuse will be given a grade of zero for that exam.

COURSE SCHEDULE

Date	Topics	Readings	Instructor
01/24	Introduction to Data Comm.	White 1	Duchessi
01/31	Fundamentals of Data and Signals	White 2	
02/07	Conducted and Wireless Media & Making Connections	White 3 & 4	
02/14	Multiplexing and Compression	White 5	
02/21	Errors, Error Detection and Error Control / Exam	White 6	
2/28	Introduction and Networking	White 7	Goel
3/6	Introduction to Security and Application Security	Schneier 1-5, 13	
3/13	Network & Wireless Security/Hacking Lab	Schneier 10-11	
3/20	Network Defense	Schneier 12	
4/3	Cryptography	Schneier 6-7, 15	
4/10	Password Security & Hacking Lab	Schneier 9 & 14	
4/17	Risk Analysis & Security Policies	Schneier 17-20, 24	
4/24	Incident Handling and Computer Forensics	Schneier 16	
5/1	Exam		

COURSE DETAILS

January 24 & 31; February 7, 14, 21
Title: Communications
Details: In this part of the course, Prof. Duchessi will cover different media types, modulation, and data transmission.

February 28, 2007
Title: Network Architecture (Wired and Wireless)
Details: This class will discuss the layers of the network (Application, Transport, Network, Link, and Physical) based on the Internet model. Important protocols of each layer are discussed as well along with the addressing scheme of the Internet. The second half the class will focus on wireless networking and students will break into teams and create their own "gumpdrop networks"

Laboratory: "Marty's Gumdrop Network" lab and assignment

March 6, 2007
Title: Introduction to Security
Topics: This class will cover the primary requirements for information security, including, confidentiality, integrity, and availability. It also covers the threats, attacks, and adversaries. In-depth coverage of application security will also be done, including, malicious code, buffer overflows and web security. The class discusses some of the modern malicious codes including, spyware, adware, and Trojans.

Laboratory: The laboratory exercises will include tools and resources to detect malicious code on the computer. In addition spyware such as keyloggers will be covered.

March 13, 2007
Title: Network and Wireless Security
Topics: This class focuses on network-based attacks such as spoofing, session hijacking, denial-of-service, and botnets as well as the mechanisms for protection against these attacks.

Laboratory: Students will conduct a network monitoring/hacking lab using open-source tools

March 20, 2007
Title: Network Defense/ Configuring a Firewall
Topics: This class will discuss different security mechanisms such as firewalls and intrusion detection systems. It will also discuss honeynets, virtual private networks and demilitarized zones. In addition, a brief introduction to cryptography will be provided in the class.

Laboratory: The laboratory exercises will include installing and deploying a firewall and intrusion detection system on a computer and configuring it.

April 3, 2007
Title: Cryptography
Topics: This first part of the class will focus on use cryptography for security implementation. It will also include message digests, message authentication codes and one-way has functions. In addition, the public key infrastructure will be discussed which will include digital signatures, digital certificates, and key exchanges.

Laboratory: Decryption in-class assignment

April 10, 2007
Title: Password Security & Hacking Lab
Topics: This class will include authentication based on passwords. It will cover different algorithms to make passwords secure as well as ways to store and retrieve passwords.

Laboratory: In this lab, students will use tools to analyze and crack passwords on Windows machines. The students will learn to access the file system using Linux-based utilities without having the passwords for the machine.

April 17, 2007

Title: Risk Analysis & Security Policies

Topics: This class covers the basic elements of risk analysis including assets, threats, controls, and vulnerabilities. A methodology to conduct risk analysis will be discussed in class and several small cases will be done in the class. The students will then break into groups and work on a risk analysis case using the methodology discussed in the class.
This class will discuss the role of security policies in an organization as well as the structure and syntax of the policies. In addition structure of a security policy as well as the components will be discussed for a specific policy (e.g. Data Classification). The class will cover some of the key government legislation that impacts the security policies in an organization (e.g. HIPAA, Sarbanes-Oxley, FERPA etc.). In the second half of the class students will work on developing a security policy based on a given scenario or analyzing a case related to security policy

Laboratory: Case Analysis

April 24, 2007

Title: Incident Handling and Computer Forensics

Topics: This class discusses handling computer incidents and analyzing computer crime. This will cover both legal as well as technical aspects of forensics. The class will cover collection of evidence, tracing of email and Internet as well as file system analysis.

Laboratory: Forensics lab using an open source tool.

May 1, 2007

Title: Conclusion

Topics: This is the final class of the semester that will wrap up the course and will also include the second module exam.