

ITM 416/604: Data Communications, Networks, and Security: Part II
University at Albany, State University of New York
Spring 2007 Syllabus

Instructor Information

Name: Sanjay Goel
Email: goel@albany.edu
Phone: 442-4925
Office Location: BA310b
Office Hours: M 12:30pm - 2:00pm or by appointment

Class Information

Time: TH 8:30am – 11:30pm
Location: BA 233
Dates: January 25 - May 3
Credit(s): 3 Call #: 6874(416) / 3913(604) Available Lab(s): HRIS and MIS Labs

WebCT (Duchessi): <http://webct.albany.edu:8900>

Website (Goel): <http://www.albany.edu/~goel/classes/spring2007/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 (Duchessi)- Data Communications & Computer Networks: A Business Users's Approach, Fourth 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

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. Due to strong demand for risk analysis and security policies the course this year is being taught in conjunction with one credit classes in risk analysis and security policies. The emphasis in the class on these two topics has consequently diminished some what and other interesting things have been added. Students who are taking those classes will get a very strong overview of these fields and would be doing supplementary work in two corresponding classes in the syllabus. The new material added to the class this year is network simulation using ns-2 as well as security tools such as firewalls and intrusion detection systems.

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 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:

Assignments- 15% (416) / 10% (604)

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% (416) / 20% (604)

The project will involve performing a risk analysis based on a case or on their own organization 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% (604 ONLY)

The paper should be done in pairs or individually with NO MORE THAN 2 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 and provide the professor with a listing of your contributions. 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. Groups of students will discuss potential topics with the professor on the first day to determine a final paper topic. Please see the Projects/Papers section of the course site for further details and guidelines.

Exam 60% (416) / 50% (604)

This 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 this part of the class 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.

COURSE SCHEDULE

Date	Topics	Readings	Assignments	Instructor
3/01	Exam	Notes	Paper Topics Assigned	GOEL
	Introduction to Module II	Notes		
3/08	Security Fundamentals	Schneier 1-5, 8		
	Application Security	Schneier 10 & 13		
3/15	Network Security & Hacking Lab	Schneier 11		
	Wireless Security & Hacking Lab	Tutorial		
3/22	Network Defense	Schneier 12	Paper Due/ Project Assigned	

Date	Topics	Readings	Assignments	Instructor
	Configuring a Firewall	Tutorial		
3/29	Risk Analysis	Schneier 6, 7 & 15		
	Case Analysis	Schneier 9		
4/12	Cryptography	Scheier 17-19		GUEST
	Password Security & Hacking Lab	Class Handouts		
4/19	Security Policy	Schneier 20	Project Due	GOEL
	Case Analysis	Class Handouts		
4/26	Incident Handling and Computer Forensics	Schneier 24 & 25		
	Review			
5/3	Conclusion / Exam	Notes & Book		

COURSE DETAILS

March 1, 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 configure their own wireless routers.

Laboratory: Configuring wireless routers

March 8, 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 15, 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 22, 2007

Title: Network Defense

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.

March 29, 2007

Title: **Risk Analysis**

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.

Laboratory: Risk analysis case

April 12, 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 hash functions. In addition, the public key infrastructure will be discussed which will include digital signatures, digital certificates, and key exchanges. The second part of the class will include authentication based on passwords. It will cover the 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 19, 2007

Title: **Security Policy**

Topics: 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: Drafting Security Policy / Analyzing a case

April 26, 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 3, 2007

Title: **Conclusion**

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