ITM 416: Data Communications, Networks, and Security
University at Albany, State University of New York
Spring 2010 – Syllabus

Instructor Information

Name: Sanjay Goel Email: goel@albany.edu Phone: 442-4925 Office Location: BA310b Office Hours: W 4-5pm, TH 1:00 – 2:30pm (or by appt.)	Name: Peter Duchessi Email: p.duchessi@albany.edu Phone: 442-4945 Office Location: BA312 Office Hours: By appt. usually after class, 11:30am – 2:30 pm

Class Information
Time: Wednesday 1:15 – 4:05 PM
Location: BA 233 / BA 222
Dates: January 20 – April 28
Credit(s): 3
Call #: 10396
Available Lab(s): 2nd Floor Business School Computer Lab

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 data communications and computer networks (OSI/Internet Model, Protocols, architectures, switching and routing schemes) and how to design a secure network including selection of communication media
2. Secure authentication topics (Asymmetric & Symmetric Cryptography, PKI, Digital Signatures & Certificates)
3. How to use penetration testing and system utilities to test for / audit against information security threats and determination of relevant controls
4. How to perform a risk assessment/analysis to evaluate security exposure and write security policies.
5. Critical thinking skills via debates on the ethics and legal issues related to information technology

ASSESSMENT & GRADING

Academic Integrity Compliance: Students MUST comply with all University standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** If a student is discovered to NOT comply with academic integrity standards, the student will be reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive either a warning, be told to rewrite the plagiarized material, receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Examples of violations include: Giving or receiving unauthorized help before, during, or after an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), Submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being (and has in the past been) submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (for example, the words, ideas, information, code, data, evidence, organizing principles, or style of presentation of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, the purchase of prepared research, papers, or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations.

If you ever have any questions about whether you could be violating academic integrity standards – ASK!

Grading Rubric

Assignments (Goel) - 20%: Assignments can be in-class or take-home and will be designated as individual or group assignments depending on the specific assignment. The assignments will be provided in class and/or through the course website or Blackboard. Assignments include hands-on laboratory exercises, performing a risk analysis based on a simulated case using the risk analysis methodology presented in class, and/or writing a small security policy. Please see the Assignments section of the course website for more details.

Exam I (Duchessi) - 30%: This exam will be an objective type exam that will cover the communications part of the class.
Exam II (Goel) - 25%: This exam will consist of multiple sections (essay-style) and will cover material from classes on 2/24, 3/3, 3/10, 3/17

Exam III (Goel) - 25%: This exam will consist of multiple sections (essay-style) and will cover material from classes on 3/24, 4/14, and 4/21, however, you will need a background from the previous portion to effectively answer questions in this exam.

"GREAT" EXPECTATIONS

- Students are expected to complete all assignments and readings as well as attend office hours as necessary. It is important for students to inform the instructor if all available office hours interfere with other classes during the first week of class.
- Students are expected to respectfully participate in class and communicate with the instructor if there is confusion or lack of understanding of the material. In turn, the instructor will attempt to clarify any material either in-class or outside of class.
- Students can expect assignments to be graded fairly and be returned within a reasonable time period with relevant comments and for the grader to be available to discuss questions. Students are expected to set up an appointment to meet with the grader within a week of receiving an assignment, project, or exam grade to discuss any related questions.
- Students who submit late assignments (out-of-class ONLY), projects, or papers can expect to lose 10% off per day late from the final possible grade for the exercise unless an excuse is legitimate. The lowest in-class assignment grade will be dropped.
- If the instructor is unable to attend class or office hours due to a personal If the instructor is unable to attend class or office hours due to a personal emergency, students can expect for arrangements to be made for an alternate instructor or to be informed in as a timely a manner as possible via email/phone.

- Students are expected to contact the Disabled Student Services Center and the relevant professor at the beginning of the semester and at least a week before each exam if they require additional assistance during test-taking.
- Students who do not show up to take an exam and do not have an excuse approved by the Dean of Undergraduate Studies office should expect to receive a grade of zero for that exam. Exams are expected to be closed-book unless otherwise specified by the instructor and students are expected to keep all personal electronic devices (laptops, cell phones, PDA's, etc.) stowed during exams.
- The syllabus is subject to change and students are expected to be aware of any modifications to the syllabus including, but not limited to: due dates, readings, exam dates, and project guidelines, either announced in-class and through email. The instructor is expected to get approval of the entire class prior to making any changes regarding the grading rubric.
- Students are expected to provide reliable contact information and inform the instructor of any updates to this information. Students are expected to contact the instructor via email, phone, or in person for reliable response. Blackboard will NOT be considered a reliable communication method.
- Students can expect the instructor to be open to questions and concerns, but remain impartial and fair to all students.

COURSE SCHEDULE

Date	Topics	Readings	Instructor
01/20-02/20	Data Communications & Networking, Exam I	White 1-6	Duchessi
2/24	Introduction & Network Architecture (Wired and Wireless)	Notes	Goel
3/3	Introduction to Security / Application Security	Schneier 1-5, 13	
3/10	Network & Wireless Security / Hacking Lab	Schneier 10-12	
3/17	Cryptography	Schneier 6-7, 15	
3/24	Risk Analysis & Security Policies	Schneier 9 & 14	
4/7	Exam II		
4/14	Password Security & Hacking Lab	Schneier 17-19, 20, 24	
4/21	Incident Handling and Computer Forensics	Schneier 16	
4/28	Exam III		

COURSE DETAILS

January 20 – February 20, 2010
Title: **Data Communications & Networking, Exam I**
Details: In this part of the course, Prof. Duchessi will cover different media types, modulation, and data transmission.

February 24, 2010
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 3, 2010
Title: **Introduction to Security / Application 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 10, 2010
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. This class will also discuss different security mechanisms such as firewalls and intrusion detection systems. It will also discuss honeynets, virtual private networks and demilitarized zones.

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

March 17, 2010

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

March 24, 2010

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 7, 2010

Title: **Exam II**

April 14, 2010

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 21, 2010

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.

April 28, 2010

Title: **Exam III**