1. Announcements

The class will meet in Robinson Hall, Rm A249 on Mondays, 7:20 – 10:00 p.m., beginning on August 31st, 2009. The specific class meeting days are provided below in section 10. The Final Exam is scheduled for Monday December 21st, 2009, from 7:20 – 10:00 p.m.

2. Expected Background

Students are expected to be familiar with basic network technology. The course is designed as an introductory element treating network security issues in more depth. If you are a student with a disability and you need academic accommodations, please see me and contact the Disability Resource Center (DRC) at 993-2474. All academic accommodations must be arranged through the DRC.

3. Expected Learning Experience

An introduction to the full spectrum of network security. Topics include Taxonomy - language commonality in incident handling; National Strategy to Secure Cyberspace; Cybersecurity Organizations - organizational structure for network defense; Best Practices, Security Policy, Threats - actors and tools, countermeasures, vulnerability identification/correction, intrusion detection, and impact assessment; Firewalls and Intrusion Detection Systems; Anti-Virus Software; Defense; Disaster Recovery; and Law Enforcement and Privacy Issues. The course reviews threats and vulnerabilities in network systems based on reports, case studies available in the literature, and actual experience.

No textbook addresses the course completely. One textbook is identified as mandatory, supplemented with on-line resources. The course will be based on lecture notes provided in PowerPoint slides and amplified with the readings. Case studies and tests will be based on these notes. The PowerPoint slides will be available to the class on a website.
4. Required Book
   A. Mandatory Textbook

   **Network Security Bible**, Cole, Krutz and Conley

   B. Supplemental readings will be discussed during lectures, but will be for those students wishing to investigate a particular subject in more depth.

5. Lecture Notes

As noted earlier, Power Point slides for the lectures will be available on a website prior to the class. The set of slides for the first class will be posted on the TCOM web site without restriction within one week of the start of classes in August. Subsequent lecture slides will be available thereafter on the class web site.

6. Homework

1. Two one-page case studies will be assigned during the semester and are due on the dates listed on the syllabus (approximately every three weeks). The format will be discussed in the first class. The third homework assignment will be based on an interactive CD (provided at class) exercise.

2. The case studies will be electronically transmitted to the instructor prior to the class date/time when it is due. Homework will be graded. **Late homework will not be accepted unless prior permission is granted. **PLEASE put your name in either the header or footer field.

3. A 7 – 10 page paper will be due two weeks prior to the final (the last class). Topic selection and format will be discussed during class. The paper will be electronically transmitted to the instructor prior to the class date/time when it is due. **Late papers will not be accepted unless prior permission is granted. **PLEASE put your name in either the header or footer field.

**IMPORTANT NOTE**

Students are encouraged to find, and use, any and every source they may locate to answer a question or for a research topic. HOWEVER: if elements of a paper or research note have been downloaded from the web or transcribed from another source, STUDENTS MUST WITHOUT FAIL acknowledge the source document. If the elements used are exact copies, those passages must be within quotation marks to note they are not original statements of the student. This includes written sections, diagrams, and pictures. Failure to acknowledge a source used is considered to contravene the copyright act and may also be subject to honor code proceedings if the student claims the work to be original when it is copied from another person or source.

7. Tests

One midterm will be given (in class) during the semester. It will be a closed book, closed notes test of about two hours. The midterm will cover class work up to and including the lecture prior to the day of the midterm. The test will come from the slides, lecture accompanying the slides as supplemented by the readings.
8. Final Exam

A closed book, closed notes final exam of about two hours will be given on Monday December 21st, 2009. The work covered in this exam will concentrate on class work after the second test, but it will also include some questions from the first part of the course.

9. Course Grades:

Final Grades will be determined by a weighted average of the case studies, the midterm, the paper, and the final exam in approximately the following manner:

- Homework: 15%
- Midterm: 35%
- Paper: 15%
- Final: 35%

10. Course Outline and Book Sections to be Covered

Lecture No. 1 August 31st, 2009
http://www.cert.org/research/taxonomy_988667.pdf),

Course Overview and a Common Language: COMPUSEC taxonomy: standardizing terminology, categorization, identification, and response.

Labor Day September 7th, 2009 – No class

Lecture No. 2 September 14th, 2009
(reading: National Strategy to Secure Cyberspace, www.whitehouse.gov and draft available at web site; Chapter 19)

Protecting the National Infrastructure: An cursory review of the published direction the US administration has chosen to safeguard national assets.

Best Practices: A review and discussion of best practices from backbone ISP perspective down to individual home user.
Lecture No. 3, September 21st, 2009

(reading: Dancho Danchev “Building and Implementing a Successful Information Security Policy” (www.WindowSecurity.com) and Chapter 2)

Security Policy: The development of comprehensive organizational policies and the importance of implementation and enforcement.

Case Study #1 due (Electronic Safety and Soundness, “The Roles of Public and Private Sectors” pp 34 – 37)

Lecture No. 4, September 28th, 2009

(reading: Chapter 4, pp 145-148, Chaper 17, pp 557-559)


Lecture No. 5, October 5th, 2009

(reading: Chapter 9 pp 326-329)


Lecture No. 6, October 13th, 2009

(reading: Chapter 13 pp 442-444; Chapter 17 pp.559-560)

Threats: DNS/BGP concept, attacks, tools, actors.

Paper topic, Case Study #2 due

Lecture No. 7, October 19th, 2009

(reading: Chapter 17 pp 560-567)

Threats: Intrusions: concepts, objectives, tools, actors.

Lecture No. 8, October 26th, 2009

(reading: Chapter 4, pp 148-149; Chapter 6, pp 218-219, 266-267; Chapter 8, pp 285-288)

Threats: Phishing, spyware/adware, spam, identity theft: tools, availability, concept, goals

Lecture No. 9, November 2nd, 2009

Midterm covering Lectures 1 - 8
Lecture No. 10, November 9th, 2009
(reading: Chapter 13; Chapter 17, pp 567-571)

Firewalls, Intrusion Detection Systems and Anti-Virus protection: tools, availability, concept, goals

Homework #3 due

Lecture No. 11, November 16th, 2009
(reading: Know Your Enemy: Defining Virtual Honeynets
Different types of Virtual Honeynets. Honeynet Project.
http://www.honeynet.org/papers/virtual/index.html
27 January, 2003 and Chapter 17, pp 573-577)

Deception Technologies: Techniques, tools and procedures to proactively respond to cyber attacks.

Lecture No. 12, November 23rd, 2009
(reading: Chapter 2, pp 59-67; Chapter 12; Chapter 17, pp 577-589)

Disaster Recovery/Continuity of Operations/Mitigation: Techniques and activities to recover from major cyber attacks. Wireless (in)Security

Lecture No. 13, November 30th, 2009
(reading: Chapter 2 pp 75-77)

Law Enforcement and Privacy Issues. Law enforcement: applicable laws, jurisdiction, forensics, international law.

Lecture No. 14, December 7th, 2009

Challenges for the Future.

7 - 10 page paper due.

Final Exam, December 21st, 2009