IST 4700 **Information Security II** Spring 2007

Instructor: Dr. Eric Swedin
Office: DV137L (at Davis campus)
Office phone: 395-3553
E-mail: eswedin@weber.edu
Web site: http://www.swedin.org/

Office Hours: 3:00-5:30 on Tuesdays and Thursdays
Other office hours are available by appointment.

Texts: Warren G. Kruse II and Jay G. Heiser, *Computer Forensics: Incident Response Essentials* (2002).
Simson Garfinkel, Gene Spafford, Alan Schwartz, *Practical Unix & Internet Security, 3rd Edition* (O'Reilly, 2003).
Linda McCarthy. *IT Security: Risking the Corporation* (Prentice Hall, 2003).

Optional texts: Ed Skoudis, *Malware: Fighting Malicious Code* (2004).
Conklin, White, Cothren, Williams, and Davis. *Principles of Computer Security* (McGraw-Hill, 2004).

Class Description:
This course covers the basic principles and concepts in information security and information assurance. It examines the technical, operational, and organizational issues of securing information systems. Topics include operating system issues, viruses, security awareness at the executive, technical and user levels, physical security, personnel security issues, policies, procedures, and the need for an enterprise security organization. Case studies and exercises in the computer lab will be used to provide examples of the need for organizations to develop security procedures and policies. Prerequisites: IST 3620 and IST 4600.

Class participation and discussion are expected. While some lecture might be presented, for the most part, the class will focus on the discussion of the assigned topics and reading.

Grading Policies: Grades will be determined on the following basis:

Quizzes	20%
Class Presentations (2)	20%
Individual Projects (4)	40%
Midterm Exam	10%
Final Exam	10%

Grades: A: 90 - 100% B: 80 - 89% C: 70 - 79% D: 60 - 69% E: 0 - 59%

Students with Disabilities:
Any student requiring accommodations or services due to a disability must contact Services for Students with Disabilities (SSD) in Room 181 of the Student Service Center on the main campus. SSD can also arrange to provide materials (including this syllabus) in alternative formats if necessary.

Exam and Assignment Policy:
Exams can be taken early, with arranged permission. Questions on all the exams will come from text readings, class lectures, and lab assignments.

Assignments are due the day shown in the schedule. You may turn them via e-mail or by hand. Late assignments are docked ten percent each week that they are overdue.

Quizzes:
There will be six quizzes, on random days. Each quiz will be based on the readings that you were given for that day. Only five quizzes will be counted, so that the lowest quiz score may be dropped.

Cheating Policy:
Cheating and deceit are not accepted in the Goddard School of Business and Economics. *Cheating on an exam or assignment, or turning in someone else's work as your own, will result in an E for the class.* You may work together on your assignments, but you must turn in your own work. If you quote from a book, article, or web site, you must properly quote and cite your work. **Avoid even the appearance of cheating or plagiarism.**

Class Presentations:
Each student will make two presentations in class. Each presentation will be accompanied with a one-page class handout, with enough copies for everyone in class. Presentations must be two on the following three categories:

1. a worm, virus, dangerous bug, or other type of malware
2. a security tool (PGP, grc.com, SecureID, etc)
3. on something interesting (DCMA, BitTorrent, hacking an X-box, Pringles can wireless receiver, RFIDs, steganography, etc)

These presentations should be specific rather than general, such as on a particular trojan horse rather than the concept of trojan horses. Each presentation should take about ten minutes. Students may not make more than one presentation a day, and cannot turn in presentations that they have not presented to the class.

These presentations may NOT duplicate material used in your previous IST 4600 course or even material that was presented by another student.

Some useful sites to find known security problems/bugs/viruses/worms:

http://www.cert.org/ - CERT Coordination Center
http://www.SecurityFocus.com/ - SecurityFocus (including Bugtraq)
http://www.vmyths.com/ - Vmyths.com - Truth About Virus Myths/Hoaxes
http://www.nipc.gov/ - National Infrastructure Protection Center (FBI)
http://www.sans.org/ - SANS Institute
http://www.w3.org/Security/Faq/www-security-faq.html - World Wide Web Security FAQ
http://www.wildlist.org/ - The WildList Organization International
http://www.hackerwatch.org/ - HackerWatch.org

Students in the past have made presentations on: instant messaging security, hacking the Playstation 2 and other console gaming systems, encryption algorithms, IP spoofing, telephone phreaking, viruses, Trojan horses, hacking satellite TV systems, TCP/IP sniffers, war dialing, war driving, wireless security, PGP, DCMA, BitTorrent, and so on. These are all still valid topics for your own presentations.

These presentations will be graded on the following criteria:

- 20% Is it new material that was not covered in class;
- 40% Quality of oral presentation;
- 40% Quality of class handout (I will take away 5% for the first grammar and spelling mistake, and then 1% for each subsequent grammar and spelling mistake).

Individual Projects:
Each student will do four individual projects out of the possible six projects below. Each project will have to be demonstrated to the instructor and you will have to submit a two-page report describing what you did (i.e., what products you used, why you used those products, what problems you encountered). Note that most of these projects require you to use two systems. **You may not do projects that you did in IST 4600.**

1) Set up a firewall and demonstrate how the firewall works by using a port scanner. Be able to explain how firewalls and port scanners work. A useful site to look at is: http://www.firewallguide.com/software.htm

2) Set up a trojan horse product on your PC and demonstrate remote control features. Examples include Sub7 and BackOrifice.

3) Set up anti-virus software on your PC and try to infect the PC with a virus or other malware.

4) Set up a sniffer and show how it tracks network traffic and be able to explain to the instructor the sniffer log.

5) Successfully hack a Windows XP or Linux machine to which you have physical access. Hacking means that you can get access to any files on the hard drive.

6) Set up an intrusion detection system (IDS) and show it catching a suspicious event, such as a denial of service attack.

7) Set up the Microsoft Security Analyzer (MSA) and demonstrate how it works. You must run it across the network against another computer.

8) Set up a honeypot or honeynet and demonstrate how it works.

9) Set up and run Security Auditor's Research Assistant (SARA) for Linux.

You will often be downloading trial versions of software and the trial period will run out. Sometimes running CyberScrub (http://www.cyberscrub.com/) can let you do reinstall trial software again.

Schedule:

Date	Thursday
January 11	Introduction to class.
January 18	*Performing Audits I.* McCarthy chapters 1-4.
January 25	*Performing Audits II.* McCarthy 5-8.
February 1	*Performing Audits III.* McCarthy 9-12; Kruse 12. Students 1-2 presentations.
February 8	*UNIX*. Kruse, 9-11. Students 3-4 presentations.
February 15	No class held.
February 22	*UNIX II.* Garfinkel, 1-3. Students 5-6 presentations.
March 1	*UNIX III*. Garfinkel, 4-6, Appendix B. Students 7-8 presentations.
March 8	**Midterm Exam** *UNIX IV.* Garfinkel, 7-9.
March 15	Spring break.
March 22	No class held.
March 29	*UNIX V.* Garfinkel, 10-13. Students 1-2 presentations.
April 5	*UNIX VI.* Garfinkel, 14-16. Students 3-4 presentations.
April 12	No class held.
April 19	*UNIX VIII*. Garfinkel, 17-22. Students 5-6 presentations.
April 26	*UNIX IX.* Garfinkel, 23-26. Students 7-8 presentations.
May 3	**Final Exam** (same time and same room as the regular class)