IST 6400 **Information Assurance for the Enterprise** 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 Tuesdays Thursdays
Other office hours are available by appointment.

Texts: Kevin D. Mitnick and William L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers* (Wiley, 2005). ISBN-13: 978-0764569593.

Linda McCarthy. *IT Security: Risking the Corporation* (Prentice Hall, 2003). ISBN-13: 978-0131011120.

Kevin D. Mitnick, *The Art of Deception: Controlling the Human Element of Security* (Wiley, 2002). ISBN-13: 978-0764542800.

Corey Schou and Dan Shoemaker, *Information Assurance for the Enterprise: A Roadmap to Information Security* (McGraw-Hill, 2007). ISBN-13: 978-0072255249.

Class Description:
This graduate course covers the basic principles and concepts in information assurance. It examines the managerial, operational, and organizational issues of securing information systems. Topics include legal and ethical issues in computer security; privacy concerns; malware; security awareness at the executive, technical and user levels; physical security, personnel security issues; policies and procedures; the need for enterprise security awareness; 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: None

Class participation and discussion are expected. While lectures and demonstrations might last one or two hours, 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:

Online Quizzes	35%
Class Presentations (3)	30%
Class Paper	20%
Class Participation	5%

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 Ogden campus. SSD can also arrange to provide materials (including this syllabus) in alternative formats if necessary.

Quizzes:
There will be seven open-book quizzes, all given online. Each quiz will be based on the readings that you were given for that week.

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 Paper:
Due on the last day of class is a ten page class paper. You may choose a topic of your choice (subject to approval by the instructor) or write about what you have learned in this course and how you will apply it.

Class Presentations:
Each student will make three presentations in class. Each student will be assigned a student number on the first day of class so that you may look on the schedule and know when you are expected to present.

Each presentation will be accompanied with a one-page class handout, with enough copies for everyone in class. You must do one presentation in each of the following three categories:

- a worm, virus, dangerous bug, or other type of malware
- a security tool (PGP, grc.com, SecureID, etc)
- 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.

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.wildlist.org/ - The WildList Organization International
http://www.w3.org/Security/Faq/www-security-faq.html - World Wide Web Security FAQ

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, 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).

Schedule:

Date	Wednesday
January 10	Introduction to class. Introduction to Information Assurance. How public keys work.
January 17	Read Mitnick, *The Art of Deception*, preface, chapters 1-5.
January 24	Read Mitnick, *The Art of Intrusion*, chapters 1-6. Students 1-5 presentations.
January 31	Read Mitnick, *The Art of Intrusion*, chapters 7-11. Students 6-10 presentations.
February 7	Read Schou and Shoemaker, chapters 1-5. Students 1-5 presentations.
February 14	Read Schou and Shoemaker, chapters 6-10. Students 6-10 presentations.
February 21	Read Schou and Shoemaker, chapters 11-16. Students 1-5 presentations.
February 28	Read all of McCarthy. Students 6-10 presentations. Class paper due.