CS 4830 (IST 4700) **Information Security II** Spring 2012

Instructor: Dr. Eric Swedin
Office: DV137L at the Davis campus
Office phone: 801-395-3553
E-mail: eswedin@weber.edu
Web site: http://www.swedin.org/

Office Hours: 12:30-5:30 on Thursdays at Davis.
Other office hours are available by appointment.

Texts: Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (2006) ISBN-10: 0387026207

Kevin D. Mitnick and William L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers* (Wiley, 2005) ISBN-10: 0471782661 ISBN-13: 978-0764569593

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.

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.

Quizzes: There will a quiz every day at the beginning of class. Each quiz will be based on the readings that you were given for that day. You may miss ONE quiz; if you take that quiz, it counts as extra credit.

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

Quizzes	40%
Class Presentation	20%
Individual Projects (2)	30%
Class participation	10%

Grades: A: 90 - 100% B: 80 - 89% C: 70 - 79% D: 60 - 69% E: 0 - 59%
(Grades at the high or low ends of these ranges will earn plus and minus grades.)

Cheating Policy: Cheating and deceit are not accepted at Weber State University. *Cheating on an quiz 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 and papers, 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.**

Individual Projects:
Each student will do these two projects. Each project will have to be demonstrated to the instructor and you will have to submit a four-page report describing what you did (i.e., what products you used, why you used those products, what problems you encountered, what security problem was solved by this project, and what security problem(s) that particular product solves).

1) Install Nessus on a Linux server and run a scan against a Linux server and a Windows server. Explain what the results mean.

3) Set up two email servers on different machines, send encrypted email from an account on one server to an account on the other server and successfully decrypt the email text.

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

Class Presentations:
Each student will make a ten minute presentation in class. The presentation will be accompanied with a one-page class handout, with enough copies for everyone in class. This presentation 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 to fifteen minutes. You may not make a presentation on a topic already covered by another student (publically claim a topic if you want to preserve it for yourself).

Students in the past have made presentations on: instant messaging security, hacking the Playstation 3 or other console gaming systems, encryption algorithms, IP spoofing, telephone phreaking techniques, hacking an iPhone, how a new example of malware works in detail, hacking satellite TV systems, new war driving techniques, wireless security, DCMA, BitTorrent issues, and so on. These are all still valid topics for your own presentations..

Campus Closure: In the event of an extended campus closure, please look at your Weber State email in order for instructions on how we will continue the class via email and the online course system.

Schedule:

Date	Thursday
January 5	Introduction to class.
January 12	Read Mitnick, *The Art of Intrusion*, chapters 4-6.
January 19	Read Mitnick, *The Art of Intrusion*, chapters 7-8.
January 26	Read Mitnick, *The Art of Intrusion*, chapters 9-11.
February 2	Read Schneier, chapters 1-2
February 9	NO CLASS; you may come and work on individual projects.
February 16	Read Schneier, chapters 3-4 Students 1-3 presentations.
February 23	Read Schneier, chapters 5-6 Students 4-6 presentations.
March 1	Read Schneier, chapters 7-8 Students 7-9 presentations.
March 8	Read Schneier, chapters 9-10 Students 10-12 presentations. **Your first project should be graded by now (I will dock 10% for each week that you are not done).**
March 15	Spring break.
March 22	Read Schneier, chapters 11-12 Students 13-15 presentations.
March 29	NO CLASS; you may come and work on individual projects.
April 5	Read Schneier, chapters 13-15 Students 16-18 presentations.
April 12	Read Schneier, chapters 16-17 Students 19-21 presentations.
April 19	**NO Final Exam**