CS 4830 **Advanced Topics in Computer Science: Information Security I** *(equivalent to IST 4600)* Fall 2012

Instructor: Eric G. Swedin, Ph.D
http://www.swedin.org/
eswedin@weber.edu
Office on Davis campus: DV137L; Office on Weber campus: SS250
Telephone: 801-395-3553 (w); 801-479-3735 (h)
Office hours: 4:30-5:30 on Mondays, Tuesdays, and Thursdays; 3:30-5:30 on Wednesdays (all at my Davis office). 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.

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

Stuart McClure, *Hacking Exposed 7 Network Security Secrets & Solutions Seventh Edition: Network Security Secrets and Solutions* (McGraw-Hill Osborne, 2012) ISBN-13: 978-0071780285.

Class Description and Objectives:
In a computer-literate age, sophisticated criminals use computers in their illegal and destructive activities. This course discusses cyber crime and teaches students how to: recognize the patterns of an impending attack; detect attacks; set up a secure environment; and use tools to investigate cyber crime. Prerequisites: IS&T Core. Co-requisite: IS&T 3620.

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 readings.

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

Quizzes	40%
Class Presentation	20%
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.)

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.

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

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

Cell Phones, Texting, and Laptops:
Put your cell phones on vibrate. Try to avoid leaving class to take a call, but an occasional emergency is understandable. There will be NO texting in this class. Laptops or other personal digital tools may be used to take notes, look up material relevant to class discussions, or for class projects. No other uses of laptops will be tolerated.

Cheating Policy:
Cheating and deceit are not accepted in the Goddard School of Business and Economics. *Cheating on a 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, 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, even in an informational handout for your fellow students. **Avoid even the appearance of cheating or plagiarism.**

Class Presentations:
Each student will make a 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.

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) Create a secured machine by doing the following:
   - The first phase of this project is to set up a firewall and demonstrate how the firewall works by using a port scanner from another machine. Be able to explain how firewalls and port scanners work. A useful site to look at is: http://www.firewallguide.com/software.htm. This site is also useful: http://www.techsupportalert.com/.
   - The second phase of this project is to demonstrate a packet sniffer to me, showing me the network traffic between the two machines, and explaining how the sniffer works and what the contents of the sniffer log mean.
   - The third phase of this project is to set up anti-virus software on your PC and try to infect the PC with a virus or other malware.
   - The fourth phase of this project is to infect your machine with a trojan horse malware product. Demonstrate the remote control features of the trojan horse. Examples include Sub7 and BackOrifice and other examples can be found at http://www.OffensiveComputing.net/.

2) Penetrate a machine by using physical access:
   - Successfully penetrate a Windows or Linux machine to which you have physical access and that is password protected. Success means that you can get access to any files on the hard drive without cracking a password.
   - The second phase of this project is to successfully penetrate a Windows or Linux machine by cracking the login password.

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 then successfully reinstall trial software again.

Schedule:

Date	Wednesday
August 30	Introduction to class. *Why Security?*
September 6	Read Mitnick, *The Art of Deception*, Preface, Introduction, chapters 1-4.
September 13	Read Mitnick, *The Art of Deception*, chapters 5-9.
September 20	*Hacking Exposed*, Case Study, Chapter 1.
September 27	*Hacking Exposed*, Chapter 2.
October 4	*Hacking Exposed*, Chapter 3. Students 1-2 presentations.
October 11	*Hacking Exposed*, Chapter 4. Students 3-4 presentations.
October 18	*Hacking Exposed*, chapter 5. Students 5-6 presentations. **First project due by this date**.
October 25	*Hacking Exposed*, Chapter 6. Students 7-8 presentations.
November 1	*Hacking Exposed*, Chapter 7. Students 9-10 presentations.
November 8	*Hacking Exposed*, Chapter 8. Students 11-12 presentations.
November 15	*Hacking Exposed*, chapter 9. Students 13-14 presentations.
November 22	*Hacking Exposed*, Chapter 10. Students 15-16 presentations.
November 29	Thanksgiving.
December 6	Read Mitnick, *The Art of Intrusion*, Preface, chapters 1-3. Students 17-18 presentations.
	No Final Exam