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 Wednesdays and Thursdays. Other office hours are available by appointment.

Texts:  

**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:

- Quizzes: 35%
- Class Presentations (2): 20%
- Class Paper: 30%
- Class Participation: 15%

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:
Starting on the second week of class, there will be a quiz every day at the beginning of class. Each quiz will be based on the readings that you were given for that week. You may miss one quiz; if you take an extra quiz, it will count as extra credit.

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 **two** 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. Use only your own words on your handouts and other papers that you submit in this class. If you quote, clearly identify through quotation marks or double-indenting what you are quoting.

Presentations can be on the following topics:
- a worm, virus, dangerous bug, or other type of malware
- a security tool (PGP, grc.com, SecureID, etc)
- on something technically 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.sans.org/ - SANS Institute
- http://sysinternals.com/ - Microsoft Windows Sysinternals (useful tools)

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.
### Schedule:

<table>
<thead>
<tr>
<th>Date</th>
<th>Wednesday</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 7</td>
<td>Introduction to class. Introduction to Information Assurance. How public keys work.</td>
</tr>
<tr>
<td>February 11</td>
<td>Read Rice, chapters 4-5. Students 1-7 presentations.</td>
</tr>
<tr>
<td>February 18</td>
<td>Read Rice, chapters 6-7, and Epilogue. Students 8-14 presentations.</td>
</tr>
<tr>
<td>February 25</td>
<td>Read all of McCarthy. Students 15-21 presentations. Class paper due.</td>
</tr>
</tbody>
</table>