USF Sarasota-Manatee College of Hospitality and Technology Leadership
CIS 3360 – 3 Credit Hours
Principles of Information Security
Summer 2014, USF Sarasota-Manatee

Instructor: Dr. Sunita Lodwig
E-Mail: slodwig@sar.usf.edu
Office Hours: Multiple formats - By Appointment

Classroom: Real-time Virtual class via Blackboard Collaborate
Time: Mondays/Wednesdays, 4:00-6:00 PM

PREREQUISITES: None.

COURSE DESCRIPTION: This course provides a broad review of the entire field of Information Security, background on many related elements, at quite a bit of detail, and hands-on exercises to facilitate an understanding of the topic as a whole. The course covers the terminology of the field, the history of the discipline, and an overview of how to manage an information security program.

COURSE TOPICS:
This course will cover the following content areas:

- The broader field of Information Security and its need in today’s business environment.
- The several threats facing any organization and the current legislation, regulation, and common ethical expectations and constraints.
- Current policies, procedures, and security mechanisms and their inherent risks. Share and review best business practices and standards of due care and diligence.
- The planning process that supports business continuity, disaster recovery, and incident response, and the use of technologies to segregate the organization from the insecure Internet.
- The various categorizations of firewall technologies and their architectures, as well as the concept of intrusions and related technologies providing an additional layer of defense.
- Public Key Encryption systems and cryptography-based protocols used in secure communications.
- The elements critical to successful implementation of an information security program.

COURSE OBJECTIVES: This course is an introduction to the field of Information Security. As such it gives an overview of the vast security landscape. It follows structured to follow a model called the Security Systems Development Life cycle (or SecSDLc), a methodology that can be used to implement information security in an organization that has little of no formal information security in place. This structure provides a theme that will guide students through an examination of the various components of the vast number of information domains of information security.

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY MISSION STATEMENT: The mission of the Information Technology Program is to provide high quality educational opportunities for students interested in pursuing careers in the broad range of fields that support our computer/information-based society and economy. Additionally, the goal is to utilize the resources of the program to provide service to society; and to emphasize to students the need for lifelong learning, to have ethical conduct, and an understanding of the diverse social context in which Information Technology is practiced.

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY PROGRAM LEARNING OUTCOMES (PLOs):
1. Demonstrate technical knowledge and skill sets (computational and analytic) needed for success in careers related to Information Technology.
2. Demonstrate an understanding of professional ethics in the development and application of Information Technology.
3. Design and develop computer processes and systems of advanced complexity.
4. Assess the potential value of new technologies and see possibly beneficial applications.
5. Conduct computer research, organize a structured presentation, and deliver it in a way that communicates to novice users as well as computer experts.
COURSE STUDENT LEARNING OUTCOMES:
Upon completion of this course, students will be able to:

- Describe the broader field of information security by defining key terms and essential concepts.
- Explain the business drivers that are propelling the increased interest in information security.
- Discuss the various threats facing organizations and the process of prioritizing them for the security planning process.
- Outline the current legislation, regulation, and common ethical expectations that constrain an organization’s options.
- Explain how to conduct an initial risk assessment with regard to security mechanisms in place and policies an procedures.
- State best business practices and standards of due care and diligence as inputs to the development of security policy including the major components, scope and target audience for each of the levels of the policy.
- Describe the planning process that supports business continuity, disaster recovery, and incident response, including when to involve outside law enforcement agencies.
- Explain the perspective on the configuration and use of technologies designed to segregate the organization from the insecure Internet.
- State the various definitions and categorizations of firewall technologies and the architectures under which firewalls may be deployed.
- Explain the concept of intrusions and the technologies needed to prevent, detect, react, and recover from such intrusions.
- Discuss the role of asymmetric systems as the foundation of Public Key Encryption systems.
- Describe the cryptography-based protocols used in secure communications (SHTTP, SMIME, SET, SSH)
- State the elements critical to successful implementation of an information security program.

TEXT AND MATERIALS

A.
Michael E. Whitman - Ph. D., CISM, CISSP, Herbert J. Mattord - MBA, CISM, CISSP
Principles of Information Security
ISBN: 1111138214

Note: I believe an ebook available for the 4th edition can be rented for $47.49 at this link:
http://www.coursesmart.com/9781111138219?__professorview=false&__hdv=6.8

B. Suggested Supplementary Materials:
www.informationsecurity.techtarget.com
www.sans.org/rr
www.ftc.gov/infosecurity
www.issa.org

The course requires students to use the internet extensively for investigative purposes as well as some lab exercises – several other web-sites will be shared in class.
INSTRUCTIONAL METHODOLOGY
The Canvas on-line course tools package, which may be accessed from campus computer labs and via the Internet at https://my.usf.edu, will be used to enhance the course. All that is required is Internet access and a reasonably up-to-date web browser. Except for response speed, there should be no difference in functionality between accessing from a lab and from home. Any exceptions to this will be announced as they become apparent. If you are new to Canvas, please review the Canvas tutorials at: www.sarasota.usf.edu/CampusComputing/Documents/CC_Student_Resources.php

If you need technical assistance with Canvas, the following two modes of help are available:
- Toll-free Helpline: 866-974-1222
- Live online help: http://usfsupport.custhelp.com/cgi-bin/usfsupport.cfg/php/enduser/chat.php

OFFICE HOURS
By appointment! We can meet face-to-face at school in my office, or we can meet in a virtual office via CANVAS or Skype. Best way to contact me is via email. Please send course-related email from Canvas only. I receive close to a 100 messages a day, and it is very easy for important emails to get buried. Email from Canvas is separate and is easier and faster to respond to! In case you need to reach me very quickly, my home phone number is 941-966-1260.

GRADING, EVALUATION AND ATTENDANCE POLICIES:
Student performance will be evaluated based on in-class participation (or via the Discussion Board), two tests, exercises, and assignments as detailed below. Late assignments will be accepted but only upto a point. Once an assignment has been discussed in class, it will no longer be accepted. Also, please note, late assignments will be penalized by a loss of 5 points (could be as much as 25% of the grade).

Below is a summary for the determination of the final grade and an explanation for each component:

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Percentage of grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exams (2)</td>
<td>40%</td>
</tr>
<tr>
<td>Quizzes, Assignments, Class Participation (class, online)</td>
<td>50%</td>
</tr>
<tr>
<td>In-Class/DiscussionBoard participation/In-class presentation</td>
<td>10%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

A grade will be determined based on the total of possible points earned, as follows: A = 90-100; B = 80-89; C = 70-79; D = 60-69; F = 59 or below

**Exams – 40%**
There will be two (2) exams, a Midterm and a Final. Each will be worth 10% of your grade (20% in all). Exams will not be cumulative – each will cover the topics covered prior to the exam, although an understanding of earlier material may be necessary as background. There will be no makeup exams. Exceptions on medical grounds will require a doctor’s letter, which will be verified by the appropriate department personnel.

**Quizzes, Assignments, and Participation – 50%**
These will account for 60% of your grade. All work should be submitted on time, by midnight of the due date. Late submissions will be penalized (or not accepted for some assignments, as announced). Dates for quizzes cannot be provided in advance, as they may occur as we complete relevant course topics.

**Participation/Presentations – 10%**
Each student will research, prepare and present one individual presentation, which together will account for a total of 20% of your grade. These presentations must include at least three (3) outside references documented in footnotes and a reference page. Students should turn in a copy of their notes, including a bibliography, or include the information in their visuals. Potential topics may be brainstormed in class; the class may actively participate in deciding what presentations they do. Presentations will be evaluated on quality, content, delivery and audience response.

You are expected to frequently review the Canvas discussion function and take part in discussions of assigned
topics. It is anticipated that there will be several discussion topics during the course, with announced (and possibly overlapping) participation timeframes. Participation that occurs after the closing participation date for a topic will not be counted for credit!

**Extra Credit**
Some assignments, exams and other activities may have an extra credit component associated with them. Points earned in this manner will not be included in the assignment or exam grade or in the final course average. They will be considered after course letter grades have been tentatively assigned and may result in an increase in your final letter grade, especially in borderline situations, and will never reduce your grade.

**Incomplete Grade**
An incomplete grade is reserved for those with good reason for having missed a small amount of work, and must be agreed by the student and instructor during the course as circumstances require. Otherwise, exams not taken or assignments not turned in will receive a zero grade and will be counted in the final grade accordingly. Please note that it is the student’s responsibility to ensure that work is completed before the end of the following semester and the Incomplete changed to a regular grade. If this is not done before the end of the following semester, the Incomplete automatically becomes an F.

**Attendance Policy**
CLASS ATTENDANCE IS OPTIONAL. Attendance is automatically recorded by Elluminate. Due to the highly interactive nature of the course and its subject matter, students are strongly encouraged to attend the live sessions. Material covered in class will not necessarily be contained in the textbook. Falling behind in assignments will affect students’ grades. Students are responsible for material covered in class, any announcements, schedule changes, etc. Absenteeism is not an excuse for late work or missed exams unless approval from your Instructor is obtained in advance. Sessions are recorded and will be made available to students after the class.

**Academic Disruption:**
The University does not tolerate behavior that disrupts the learning process. The policy for addressing academic disruption is included with Academic Dishonesty in the catalog: [www.ugs.usf.edu/catalogs/0607/adapad.htm](http://www.ugs.usf.edu/catalogs/0607/adapad.htm). The consequences to the student can range from an administrative reprimand to suspension from USF.

**The last day to drop a course with a grade of “W” is ???. There will be no refund and no academic penalty.**

**USFSM Policies**

A. **Academic Dishonesty:** The University considers any form of plagiarism or cheating on exams, projects, or papers to be unacceptable behavior. Please be sure to review the university’s policy in the catalog, [USFSM Undergraduate Catalog](http:// catalogs.usf.edu/undergraduate) or [USFSM Graduate Catalog](http://catalogs.usf.edu/graduate), the USF System Academic Integrity of Students, and the [USF System Student Code of Conduct](http://studentconduct.usf.edu).

B. **Academic Disruption:** The University does not tolerate behavior that disrupts the learning process. The policy for addressing academic disruption is included with Academic Dishonesty in the catalog: [USFSM Undergraduate Catalog](http://catalogs.usf.edu/undergraduate) or [USFSM Graduate Catalog](http://catalogs.usf.edu/graduate), USF System Academic Integrity of Students, and the [USF System Student Code of Conduct](http://studentconduct.usf.edu).

C. **Contingency Plans:** In the event of an emergency, it may be necessary for USFSM to suspend normal operations. During this time, USFSM may opt to continue delivery of instruction through methods that include but are not limited to: CANVAS, Blackboard Collaborate, Skype, and email messaging and/or an alternate schedule. It’s the responsibility of the student to monitor CANVAS site for each class for course specific communication, and the main USFSM and College websites, emails, and [MoBull](http://mobull.usf.edu) messages for important general information. The USF hotline at 1 (800) 992-4231 is updated with pre-recorded information during an emergency. See the [Safety Preparedness Website](http://preparedness.usf.edu) for further information.

D. **Disabilities Accommodation:** Students are responsible for registering with the Office of Students with Disabilities Services (SDS) in order to receive academic accommodations. Reasonable notice must be given to
the SDS office (typically 5 working days) for accommodations to be arranged. It is the responsibility of the student to provide each instructor with a copy of the official Memo of Accommodation. Contact Information: Disability Coordinator, 941-359-4714, disabilityservices@sar.usf.edu; http://www.usfsm.edu/students/disability.

E. **Fire Alarm Instructions:** At the beginning of each semester please note the emergency exit maps posted in each classroom. These signs are marked with the primary evacuation route (red) and secondary evacuation route (orange) in case the building needs to be evacuated. See Emergency Evacuation Procedures.

F. **Religious Observances:** USFSM recognizes the right of students and faculty to observe major religious holidays. Students who anticipate the necessity of being absent from class for a major religious observance must provide notice of the date(s) to the instructor, in writing, by the second week of classes. Instructors canceling class for a religious observance should have this stated in the syllabus with an appropriate alternative assignment.

G. **Web Portal Information:** Every newly enrolled USF student receives an official USF e-mail account. Students receive official USF correspondence and CANVAS course information via that address.

**GENERAL INSTRUCTION FOR STUDENTS**

Students are not permitted to take notes or tape lectures for the purpose of sale. This includes Elluminate recordings.

Microsoft Office may be used to supplement this course. The online course tools package, which may be accessed from campus computer labs and via the Internet at https://my.usf.edu, will be used to enhance the course. Internet access and a reasonable up-to-date web browser are required. Except for response speed, there should be no difference in functionality between accessing from a lab and from home. Any exceptions to this will be announced as they become apparent.

**COURSE SCHEDULE:** Please note this is a tentative schedule – some shifting could occur as we progress into the semester.

<table>
<thead>
<tr>
<th>Week #/Start Date</th>
<th>Topic</th>
<th>Lab Work/Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wk 1 – May 11</td>
<td>Chapter 1 - Introduction to Information Security</td>
<td></td>
</tr>
<tr>
<td><strong>Security Investigation Phase</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wk 1 – May 11</td>
<td>Chapter 2 - The need for security</td>
<td>Assignment 1</td>
</tr>
<tr>
<td>Wk 2 – May 18</td>
<td>Chapter 3 - Legal, Ethical and Professional Issues</td>
<td></td>
</tr>
<tr>
<td><strong>Security Analysis and Planning – Risk Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wk 2 – May 18</td>
<td>Chapter 4 – Risk Management</td>
<td>Assignment 2</td>
</tr>
<tr>
<td>Wk 3 – May 25</td>
<td>Chapter 4 – Risk Management</td>
<td></td>
</tr>
<tr>
<td>Wk 4 – May 25</td>
<td>Chapter 5 - Planning for Security</td>
<td>Assignment 3 - Lab Ex. – Footprinting</td>
</tr>
<tr>
<td>Wk 4 – June 1</td>
<td>Chapter 5 - Planning for Security</td>
<td></td>
</tr>
<tr>
<td><strong>Security Technology</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Week</td>
<td>Chapters</td>
<td>Assignments</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Wk 4 – June 1</td>
<td>Chapter 6 – Firewalls and VPNs</td>
<td>Assignment 4</td>
</tr>
<tr>
<td>Wk 5 – June 8</td>
<td>Chapter 6 – Firewalls and VPNs</td>
<td></td>
</tr>
</tbody>
</table>

**End of Week 5: MID-TERM (Based on Chs 1 – 5)**

<table>
<thead>
<tr>
<th>Week</th>
<th>Chapters</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wk 5 – June 8</td>
<td>Chapter 7 - Security Tools</td>
<td></td>
</tr>
<tr>
<td>Wk 6 – June 15</td>
<td>Chapter 7 - Security Tools</td>
<td></td>
</tr>
<tr>
<td>Wk 6 – June 15</td>
<td>Chapter 8 - Cryptography</td>
<td>Assignment 5 - Lab Ex. - Scanning &amp; Enumeration</td>
</tr>
<tr>
<td>Wk 7 – June 22</td>
<td>Chapter 8 - Cryptography</td>
<td></td>
</tr>
<tr>
<td>Wk 7 – June 22</td>
<td>Chapter 9 - Physical Security</td>
<td>Assignment 6</td>
</tr>
<tr>
<td>??</td>
<td>Last day to Withdraw from Course</td>
<td></td>
</tr>
<tr>
<td>Wk 8 – June 29</td>
<td>Chapter 10 - Implementing Security</td>
<td></td>
</tr>
<tr>
<td>Wk 8 – June 29</td>
<td>Chapter 10 - Implementing Security</td>
<td>Assignment 7 - Lab Ex. - OS Vulnerabilities &amp; Resolutions</td>
</tr>
<tr>
<td>Wk 9 – July 6</td>
<td>Chapter 11 - Security and Personnel</td>
<td></td>
</tr>
<tr>
<td>Wk 9 – July 6</td>
<td>Chapter 12 - Maintenance</td>
<td>Lab Ex. - Network Security Tools &amp; Technologies</td>
</tr>
<tr>
<td>Wk 10 – July 13</td>
<td>Chapter 12 - Maintenance</td>
<td></td>
</tr>
</tbody>
</table>

**End of last Week of semester: FINAL TEST (Based on Chs 6-12)**

---

**White Hat Oath and Agreement**

Along with this syllabus is an Ethics Statement known as the White Hat Oath (available on Canvas). Please study this document and be prepared to sign the Agreement. The Agreement states that you will not use the information learned to perform unauthorized examinations of systems and information both inside and outside the University. You must sign this agreement in order to participate in the laboratory portion of this course.