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

Instructor: Mr. Jeremy L. Rasmussen, CISSP, CEH, PMP  
E-Mail: jrasmuss@cse.usf.edu  
Office Hours: After class on Mondays or by other appointment  

Classroom: Virtual class via Blackboard Collaborate  
Time: Mondays, 6:00-8:50 pm

PREREQUISITES: Consult your Advisor for the latest prerequisites.

COURSE DESCRIPTION: This course provides important foundational principles for securing vital information and reducing risk. It covers basic access control, identity management, and cryptography concepts, as well as emerging security concerns in cloud computing, mobile computing, and industrial controls (SCADA).

COURSE TOPICS:
This course will cover the following content areas:
1. Risk management
2. Assessing network security
3. Devices and infrastructure security
4. Access control
5. Wireless networks
6. Cloud security
7. Host and application security
8. Cryptography
9. Malware
10. Social engineering
11. Security administration
12. Disaster recovery and incident response

COURSE OBJECTIVES: This course is intended to provide students with an understanding of information security that will enable them to apply the most effective protections in securing valuable information assets. These topics provide the foundational knowledge to enable students to pass the CompTIA Security+ exam SY0-401. Note that CompTIA provides the Security+ examination. This course will assist students in preparing for this certification exam.

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:
1. Understand current trends in information security
2. Understand the basic Security Services
3. Understand the nature of cybersecurity attacks
4. Understand and apply basic Cryptanalysis techniques
5. Understand and apply symmetric cryptography techniques and have familiarity with common ciphers
6. Understand access control techniques and models
7. Understand application-based attacks and countermeasures
8. Understand the basics of networks, networking protocols, and attacks/countermeasures against networks
9. Understand firewalls, intrusion detection, and intrusion prevention systems
10. Understand and apply risk assessment and mitigation techniques

TEXT AND MATERIALS

A. Texts: The recommended textbook for this course:
Emmett Dulaney, Chuck Easttom
ISBN: 978-1-118-87507-0
552 pages
Published: May 2014

B. Suggested Supplementary Materials:
USF Whitehatters Computer Security Club (WCSC): If you are serious about information security and want more hands-on learning outside the classroom environment, consider joining WCSC. The purpose of the club is to promote learning about computer security and participate in organized Capture the Flag (CtF) events. The club meets weekly on Fridays at 5 p.m. in the Marshall Center, on the Tampa campus. Site: www.whitehatters.org.

GRADING, EVALUATION AND ATTENDANCE POLICIES:
Student performance will be evaluated based on tests, exercises, assignments and projects, as detailed below. All assignments are expected to be turned in on time, by 6:00 p.m. of the date assigned. They must be submitted via Canvas (not email). Late assignments will not be accepted unless prior permission has been granted by your Instructor. Each assignment will be reviewed in class after the Due Date.
Below are 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>Tests</td>
<td>30%</td>
</tr>
<tr>
<td>Quizzes, Assignments, Class Participation (class, online)</td>
<td>20%</td>
</tr>
<tr>
<td>Team Project</td>
<td>20%</td>
</tr>
<tr>
<td>Test 2</td>
<td>30%</td>
</tr>
<tr>
<td><strong>Total</strong></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

**Tests – 60%**
There will be two tests. Each will be worth 30% of your grade (60% in all). Tests will not be cumulative – each will cover the topics covered prior to the test, although an understanding of earlier material may be necessary as background. There will be no makeup tests. Exceptions on medical grounds will require a doctor’s letter, which will be verified by the appropriate department personnel.

**Quizzes, Assignments, and Participation – 20%**
All work should be submitted on time, by 6:00 p.m. 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. There will be about 5-6 of these assignments during the semester.

**Team Project – 20%**
Students will collaborate on teams of 2-4 to perform research and development of cybersecurity solutions. All projects will include a detailed written technical report, research that includes literature search, and complete listings and output (as applicable) of any custom code, tools, or scripts developed for the project.

**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**
There is a live lecture on Mondays from 6:00 – 8:50 p.m. using the Blackboard Collaborate feature of Canvas. All lectures are recorded for viewing at your convenience. I will also post PowerPoint slides for the lectures each week. Students are encouraged to connect to the live lectures on Tuesdays. Part of the student’s grade is based on class participation, which is difficult if the student is only watching the recorded conference sessions offline. There are some other opportunities for participating, such as the class discussion board, but these do not take the place of the live lecture and discussion. It is my experience that students who participate in the live session historically perform better in the class than those who do not.

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.

**USFSM Policies**
- **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 or USFSM Graduate Catalog, the USF System Academic Integrity of Students, and the USF System Student Code of Conduct.
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](#) or [USFSM Graduate Catalog](#), USF System Academic Integrity of Students, and the [USF System Student Code of Conduct](#).

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](#) 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](#) 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](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 Blackboard Collaborate 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](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.

Week 1, August 25 – **Course Introduction, Digital Threats**
Course overview
Discussion of assignments, grading format, class project
What are Information Systems?
What is Information Systems Security? Why is it important?
What are some current trends in Info Sys Security?
What are the basic Security Services?
Week 2, Sept. 1 – The nature of attacks, types of attacks, people who attack
Risk Assessment
Quantitative vs. Qualitative
Vulnerabilities and Threats
Hacking methodology
Security measures
Vulnerability Assessments

Week 3, Sept. 8 – Monitoring and Audit
Monitoring, alerting, reporting
Continuous monitoring
Wireless filtering
Attack signatures

Week 4, Sept. 15 – Network Security, Part 1
Internet History
Network Reference Models
Protocols, Layers, Services
Wireless security
Kerberos
Single sign-on
IP, TCP, UDP, ICMP
Network attacks: IP spoofing, SYN Flood, Sequence guessing
Denial of Services attacks

Week 5, Sept. 22 – Network Security, Part 2
Virtual Private Networks (VPNs)
Firewall types
Firewall architectures
Stateful packet inspection
Anomalous behavior detection
IDS/IPS

Week 6, Sept. 29 – Access Control
Authentication systems
Identification techniques
Access control techniques
Identity management techniques
Access control models
Password security
Smart cards
Biometrics
Reading: Security+ Study Guide, Chapter 4.
Week 7, Oct. 6 – **Wireless Security**
WEP, WPA, WPA2
TKIP, MIC
Wireless security issues and mitigations
Reading: Security+ Study Guide, Chapter 5

Week 8, Oct. 13 – **Cloud Security**
Virtualization
Cloud concepts
Sandboxes
Storage in the cloud
Review for Test #1

**Test #1 – online via MyUSF**
To review for Test #1: study lecture notes, chapters 1-6 in Security+ book, homework, and any additional handouts.

Week 9, Oct. 20 – **Host and Software Security**
Application-based attacks and countermeasures Buffer overflows
Injection attacks, fuzzing techniques
Mobile security concepts
OS hardening and patch management

Week 10, Oct. 27 – **Cryptography, Part 1**
Symmetric vs. asymmetric
Block vs. stream ciphers
Hashing
Steganography

Week 11, Nov. 3 – **Cryptography, Part 2**
Application of cryptography in various scenarios (Web, email, etc.)

Week 12, Nov. 10 – **Malware and Attacks**
Malware types- virus, worm, Trojan
Types of attacks
Web/application layer attacks
Provide appropriate countermeasures

Week 13, Nov. 17 – **Physical Security and Security Administration**
Physical security controls
Social engineering techniques
Countermeasures

Week 14, Nov. 24 – **Semester Team Projects Due: Nov. 24.**
No class tonight; Thanksgiving break.
Week 15, Dec. 1 – Disaster Recovery and Incident Response
Business continuity
Forensics
Incident response
Review for Test #2

Week 16, Dec. 8
Test #2 – online via MyUSF
To review for Test #2: study lecture notes, chapters 7-12 in Security+ book, homework, and any additional handouts.