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

Instructor: Mr. Jeremy L. Rasmussen, CISSP, CEH, PMP
E-Mail: jrasmuss@cse.usf.edu
Office Hours: By appointment; just email me.

Classroom: Virtual class via Blackboard Collaborate
Time: At your own pace

PREREQUISITES: Consult your Advisor for the latest prerequisites. I recommend some computer literacy, because this is a junior level Information Technology class. If you are not familiar with computers, operating systems, networking concepts, or any sort of programming language whatsoever – you may struggle in this course.

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.

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:

   **CompTIA Security+ Study Guide: SY0-401, 6th Edition**
   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](http://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 11:59 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. It is okay for students to work ahead and complete all assignments and tests if they desire, but no makeups or extra credit will be offered.

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>Test 1</td>
<td>25%</td>
</tr>
<tr>
<td>Quizzes, Assignments, Labs</td>
<td>25%</td>
</tr>
<tr>
<td>Team Project</td>
<td>25%</td>
</tr>
<tr>
<td>Test 2</td>
<td>25%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></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 – 50%**
There will be two tests. Each will be worth 25% of your grade (50% 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 – 25%**
All work should be submitted on time, by 11:59 p.m. of the due date. Late submissions will be penalized (or not accepted for some assignments, as announced). There will be about 5-6 of these assignments during the semester.

**Team Project – 25%**
Students will collaborate on teams of 3-4 to perform research and development of cybersecurity solutions. All projects will include detailed written and oral technical reports.

**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 no live lecture attendance requirement. All lectures will be recorded and available for playback using the Blackboard Collaborate feature of Canvas. I will also post PowerPoint slides for all of the lectures.

**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 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.

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 must 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.

H. Student Wellness: The Counseling and Wellness Center is a confidential resource where you can talk about incidents of sexual harassment and gender-based crimes including sexual assault, stalking, and domestic/relationship violence. You can receive assistance in confidence. This confidential resource can help you without having to report your situation to the Office of Student Rights and Responsibilities (OSSR) or the Office of Diversity, Inclusion, and Equal Opportunity (DIEO); unless you request that they make a report. Please be aware that educators must report incidents of sexual harassment and gender-based crimes including sexual assault, stalking, and domestic/relationship violence. If you disclose any of these situations in class, in papers, or to me personally, I am required to report it to OSSR or DIEO for investigation. The Deputy Coordinator for USFSM is Mary Beth Wallace, AVP for Student Enrollment, Engagement and Success, 941-359-4330 or marybeth@sar.usf.edu. Other number and resources:

- Counseling Center and Wellness Center 941-487-4254
- Victim Advocate (24/7) 941-504-8599

List of off-campus resources:
- Hope of Manatee: 941-755-6805
- Safe Place & Rape Crisis Center (SPARCC) – Sarasota: 941-365-1976
- First Call for Help- Manatee: 941-708-6488; Sarasota & North Port 941-366-5025
- Manatee Glens: 941-782-4800

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, 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.

Important dates:
- January 5, Spring, first day of classes
- March 21, Spring, last day to drop without academic penalty
- April 24, Spring, last day of classes
COURSE SCHEDULE:

We split the semester into two parts, A and B, each having 7 learning modules, 2 hands-on labs, 3 assignments, and 1 test. There is also a semester-long team project that is due toward the end of Part B. Students can watch the lectures and work the labs and assignments at their own pace. However, to keep everyone on track, there are certain due dates by which each assignment, lab, or test must be completed. They are roughly every two weeks. Make sure you are familiar with the assignments section on Canvas and the due dates for each. There will also be a course discussion board online where students can share and comment on pertinent issues in cybersecurity to gain extra credit.

Course Part A:

Module 1: Course Introduction, Measuring and Weighing Risk
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 Systems Security?
What are the basic Security Services?
Risk Assessment
Quantitative vs. Qualitative
Security Controls
Backups
Redundancy, RAID
Reading: Security+ Study Guide, Forward and Intro, Chapter 1.
Assignment 1: Security Video, due by 1/16/2015 at 11:59 p.m.

Module 2: Monitoring and Diagnosing Networks
System monitoring and audit
Event logs
Security hardening
Network security
Configuration management
Reporting

Module 3: Network Security, Part 1
Internet History
Network Reference Models
Protocols, Layers, Services
IP, TCP, UDP, ICMP
Network attacks: IP spoofing, SYN Flood, Sequence guessing
Denial of Services attacks

Lab 1: Understanding TCP/IP with Wireshark
Assignment 2: due by 1/30/2015 at 11:59 p.m.

Module 4: Network Security, Part 2
Firewall types
Firewall architectures
Stateful packet inspection
Routers
Switches
Proxies
IDS/IPS
Anomalous behavior detection
Spam

**Module 5: Access Control**
Network administration principles
Authentication systems
Identification techniques
Access control techniques
Identity management techniques
Access control lists
Password security
Smart cards
Biometrics
RADIUS, Kerberos
Reading: Security+ Study Guide, Chapter 4.

**Module 6: Wireless Security**
WEP, WPA, WPA2
TKIP, MIC
Wireless security issues and mitigations
Reading: Security+ Study Guide, Chapter 5

**Module 7: Cloud Security**
Virtualization
Cloud concepts
Sandboxes
Storage in the cloud

**Lab 2: Understanding Virtualization**
Assignment 3: due by 2/13/2015 at 11:59 p.m.

**Test #1 on Part A – online via MyUSF**
To review for Test #1: study lecture notes, chapters 1-6 in Security+ book, homework, and any additional handouts.
Students must take this exam no later than 2/27/2015 at 11:59 p.m.

**Course Part B:**

**Module 8: Host and Software Security**
Injection attacks, fuzzing techniques
Security coding
Mobile security concepts
OS hardening and patch management
Module 9: Cryptography, Part 1
Symmetric vs. asymmetric
Block vs. stream ciphers
Hashing
Steganography
Block ciphers
Block Cipher modes
DES, AES

Module 10: Cryptography, Part 2
Public key cryptography
RSA, Diffie Hellman
PKIs
Application of public key crypto

Module 11: Malware and Attacks
Malware types- virus, worm, Trojan
Types of attacks
Web/application layer attacks
Provide appropriate countermeasures
Reading: Security+ Study Guide, Chapter 9

Lab 3: Malware analysis
Assignment 4: due by 3/13/2015 at 11:59 p.m.

Module 12: Physical Security and Security Administration
Physical security controls
Social engineering techniques
Countermeasures

Module 13: Security Administration
Risk mitigation
Compliance
Vulnerability scanning and penetration testing

Lab 4: Vulnerability scanning and penetration testing
Assignment 5: due by 3/27/2015 at 11:59 p.m.

Module 14: Disaster Recovery and Incident Response
Business continuity
Forensics
Incident response
Review for Test #2
Assignment 6: DR/BC due by 4/10/2015 at 11:59 p.m.

→ Semester Team Projects: due by 4/17/2015 at 11:59 p.m.
Test #2 – online via MyUSF
To review for Test #2: study lecture notes, chapters 7-12 in Security+ book, homework, and any additional handouts. Students must take this exam no later than 4/22/2015 at 11:59 p.m.