UNIVERSITY OF SOUTH FLORIDA
COLLEGE OF ENGINEERING

USF Department of Computer Science and Engineering
CIS 4364 – 3 Credit Hours
Cryptology and Information Security
Spring, 2015

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

Classroom: ENB 118 (and virtually via Blackboard Collaborate)
Time: Tuesdays, 6:30 - 9:15 pm
T.A.: Renhao Liu; renhaoliu@mail.usf.edu. Office hrs. TBA

PREREQUISITES: Consult your Advisor for the latest prerequisites.

COURSE DESCRIPTION: This course teaches the basics of cryptography as method for providing confidentiality, integrity, and authentication of information systems.

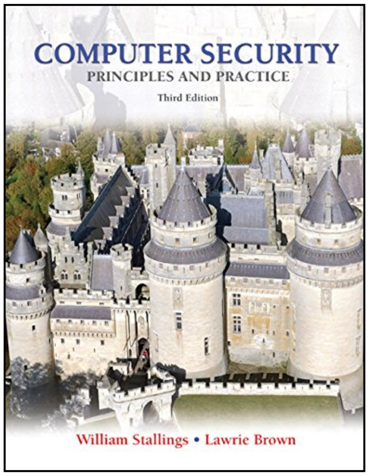
COURSE TOPICS:
This course will cover the following content areas:

1. Symmetric and asymmetric cryptography
2. Network security
3. Access control
4. Security models
5. Applications security
6. Application of cryptography
7. Risk assessment

COURSE OBJECTIVES: This course is intended to provide students with a foundational understanding of cryptography that will enable them to apply the most effective protections in securing valuable information assets. Note that in addition to a full treatment of cryptography concepts in the first half of the course, the latter half will provide the student with a survey of other information security concepts to include application of cryptography, as well as software application security, network security, and security risk management. These topics provide the foundational knowledge to enable students to pass the CompTIA Security+ exam SY0-301.

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 basic Information Theory and Complexity Theory
5. Understand and apply basic Cryptanalysis techniques
6. Understand codes, steganography, and one-time pads
7. Understand and apply symmetric cryptography techniques and have familiarity with common symmetric ciphers
8. Understand block cipher and stream cipher and cryptographic modes
9. Understand and apply asymmetric cryptography techniques and have familiarity with common asymmetric ciphers
10. Understand hashes, MACs, and HMACs
11. Understand public key infrastructures, certificates, and the application of PKI techniques to secure a variety of systems
12. Understand access control techniques and models
13. Understand application-based attacks and countermeasures
14. Understand the basics of networks, networking protocols, and attacks/countermeasures against networks
15. Understand firewalls, intrusion detection, and intrusion prevention systems
16. Understand and apply risk assessment and mitigation techniques



TEXT AND MATERIALS

A. Text: The recommended textbook for this course:
Computer Security: Principles and Practice, 3rd Ed. By William Stallings and Lawrie Brown. ISBN-13: 978-0133773927 ISBN-10: 0133773922. A tutorial and survey on network security technology. Each of the basic building blocks of network security, including conventional and public-key cryptography, authentication, and digital signatures, are covered. Mathematical background for such algorithms as AES and RSA. The book covers important network security tools and applications, including S/MIME, IP Security, Kerberos, SSL/TLS, SET, and X509v3. In addition, methods for countering hackers and viruses are explored.

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 6:30 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:

Assignment	**Percentage of grade**
Tests 1	30%
Quizzes, Assignments, Class Participation (class, online)	20%
Team Project	20%
Test 2	30%
Total	**100%**

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 6:30 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 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. Sample projects may include the following:

- Implementation/proof of a Symmetric Block Cipher
- Implementation/proof of RSA
- Implementation/proof of a secure E-Commerce Web site
- Implementation/proof of custom Steganography program

Attendance Policy

There is a live lecture on Tuesdays from 6:30 – 9:15 p.m. in ENB 118. All students are expected to attend this lecture and participate in class discussions and activities as part of their class participation grade. Since the instructor may have to travel on occasion during the semester, we may utilize the Blackboard Collaborate feature of Canvas to have virtual class sessions. These will be announced ahead of time. I will also post PowerPoint slides for the lectures each week.

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.

Classroom 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, 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 USF Undergraduate 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 USF to suspend normal operations. During this time, USF 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 USF 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.

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: General SDS Office; 974-4309 (phone); sa-sds-information@usf.edu. For exam-related issues: sa-sds-exams@usf.edu.

E. **Religious Observances**: USF 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.

F. **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, 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, Jan. 6 – **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?
Reading: Computer Security, Chapters 0.

Week 2, Jan. 13 – **The nature of attacks, types of attacks, people who attack**
Vulnerabilities and Threats
Hacking methodology
Security measures
Reading: Computer Security, Chapter 1.

Week 3, Jan. 20 – **Cryptanalysis and Classic Cryptography**
Information Theory - Claude Shannon Complexity Theory
Cryptanalysis and attacks Cryptography Basics
Codes, Steganography, and Ciphers One-time pads
Reading: Computer Security, Chapter 2.

Week 4, Jan. 27 – **Symmetric Cryptography**
Computer cryptographic algorithms—Symmetric vs. Asymmetric/Symmetric Encryption Block Ciphers
Data Encryption Standard (DES)
Advanced Encryption Standard (AES)
Cryptographic Modes
Reading: Computer Security, Chapter 20.

Week 5, Feb. 3 – **PKE, Hashes and MACs, Digital Signatures**
One-way hash functions: MD5, SHA-1
Reading: Computer Security, Chapters 21, sect. 1-2

Week 6, Feb. 10 – **Asymmetric Cryptography**
Public-key encryption RSA
Key Management Diffie-Hellman
ECC
Other public key algorithms

Reading: Computer Security, Chapter 21, sect. 3-6

Week 7, Feb. 17 – **Digital Signatures**
Digital Certificates & X.509 PKI
SSL
S/MIME
Reading: Computer Security, Chapters 22-23

Week 8, Feb. 24 – **Access Control**
Access control concepts
Authentication systems
Identification techniques
Access control techniques
TCSEC Orange Book
Common Criteria
Access control models
Password security
Smart Cards
Biometrics
Review for Test #1
Reading: Computer Security, Chapters 3-4.

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

Week 9, Mar. 3 – **Spring Break**
Work on Semester Team Projects!

Week 10, Mar. 10 – **Software Security**
Application-based attacks and countermeasures Buffer overflows Malicious code
Injection attacks
Covert channels
Reading: Computer Security, Chapters 6, 10-11.

Week 11, Mar. 17 – **Network Security**
Internet History
IETF, IESG, RFCs
Network Reference Models, Protocols, Layers, Services Wireless security
Kerberos
Single sign-on
Reading: Computer Security, Appendix F

Week 12, Mar. 24 – **Network Security**
IP, TCP, UDP, ICMP
Network attacks: IP spoofing, SYN Flood, Sequence guessing Denial of Services attacks
IETF Security Architecture (IPSEC)
Transport & Tunnel Modes
AH, ESP, SA, SPI, etc.
Key Management: ISAKMP/Oakley, SKIP
Virtual Private Networks (VPNs)
Reading: Computer Security, Appendix F, Chapt. 7, 22-24

Week 13, March 31 – **Firewalls and Intrusion Detection**
Firewall types
Firewall architectures
Stateful packet inspection
Intrusion Detection Systems
Attack signatures
Intrusion Detection Systems
Intrusion Prevention Systems
Anomalous behavior detection
Reading: Computer Security, Chapters 8-9.

Week 14, April 7 – **Forensics and Investigations**
Computer security laws
Incident response
Conducting digital forensics investigations

Semester Team Projects Due: April 7.

Week 15, April 14 – **Risk Assessment, Audit**
Vulnerability Assessments Privacy & security
Performing Security Assessments Computer crime and forensics
Other topics as time permits
Review for Test #2
Reading: Computer Security, Chapters 14, 18.

Week 16, April 21
Test #2 – online via MyUSF
To review for Test #2: study lecture notes, chapters in Stallings book, homework, and any additional handouts.