Secure Coding (CIS 4930)

CRN 92984, Section 011, 3 Credit Hours
Course Prerequisite: Data Structures (COP 4530)
College of Engineering, Department of Computer Science and Engineering

COURSE SYLLABUS

Instructor Name:	Jay Ligatti (ligatti@usf.edu)	Semester/Term & Year:	Fall 2018
Office Hours:	MW 3:30-5pm, in ENB 333	Class Meeting Times:	MW 5-6:15pm
Course website	www.cse.usf.edu/~ligatti/sc/18/	Class Location:	CHE 101A
Teaching Assistant:	Cagri Cetin (cagricetin@mail.usf.edu)	TA Office Hours:	TTh 5-6pm (ENB 325)

I. University Course Description

Principles and practices for secure computing and writing secure software, including software for performing information management and networking and communications.

II. Course Purpose

Software developers should be familiar with and understand the basic principles and practices for computing securely and writing secure software. This course covers these topics, including in the context of software for performing information management and networking and communications.

III. Course Objectives

Students having successfully completed this course will understand the basic principles and practices of secure computing and writing secure software, including: security threats, secure software design, authentication, authorization, access control, buffer-overflow attacks, type safety, layered networking architectures, basic network protocols, firewalls, intrusion-detection systems, web applications, databases and information management, SQL queries, SQL injection attacks and defenses, XSS, symmetric cryptography, asymmetric cryptography, and password management.

IV. Student Learning Outcomes

Students will demonstrate the ability to:

1. explain the basic principles and practices of secure computing and writing secure software;
2. analyze, evaluate, and explain security vulnerabilities (including buffer overflows, SQL injections, and XSS) in software designs and implementations;
3. synthesize alternative designs and implementations that incorporate mitigations for observed vulnerabilities; and
4. apply knowledge of information management and computer networking and communications while performing software-security assessments and designing and implementing secure code.

V. Required Textbook

- Foundations of Security. Neil Daswani, Christoph Kern, and Anita Kesavan. Apress, 2007 (1st ed). ISBN-10: 1590597842; ISBN-13: 978-1590597842.
  This book is accessible online from machines on the USF network:
  https://link.springer.com/book/10.1007/978-1-4302-0377-3

VI. Supplementary (Optional) Readings

- Online readings may be linked from the course webpage.

VII. Basis for Final Grade

There will be 7 tests and 1 final exam. The lowest score on a non-final-exam test will be dropped, so final grades are determined by 6 test scores (each worth 12.5% of the final grade) and 1 final-exam score (worth 25% of the final grade). *All the tests and final exam are cumulative; earlier material may appear on any test*.

The scale for final letter grades is as follows, using standard notation for ranges: A (∞,93.3], A- (93.3,90], B+ (90,87.7], B (87.7,83.3], B- (83.3,80], C+ (80,77.7], C (77.7,73.3], C- (73.3,70], D+ (70,67.7], D (67.7,63.3], D- (63.3,60], and F (60,-∞). A+ grades may be awarded for exceptionally outstanding work.

VIII. Grade Dissemination

All grades will be posted on Canvas. Tests will be returned and discussed in class.

IX. Course Policies: Grades

Late Work Policy: There are no make-ups for the tests or final exam. Your lowest non-final test score is dropped in order to allow you to miss one test without penalty, for example due to illness or an emergency.

Extra Credit Policy: This course does not generally offer extra credit, but test scores may sometimes have points added to them after grading (that is, "be curved"), depending on the extent to which the tests are challenging.

Grades of "Incomplete": An "I" grade may be awarded to a student only when a small portion of the student's work is incomplete and only when the student is otherwise earning a passing grade. The time limit for removing the "I" is to be set by the instructor of the course. For undergraduate students, this time limit may not exceed two academic semesters (whether or not the student is in residence) and/or graduation, whichever comes first. An "I" grade not removed by the end of the time limit will be changed to an "IF" or "IU," whichever is appropriate.

Essay Policy: Tests and the final exam may include one or more essay questions. Respond in complete sentences. Avoid extraneous details in your responses. Essays will be graded based on readability, correctness, and thoroughness.

(Non-)Group Work Policy: All of the tests and final exam in this course are closed books, notes, computers, phones, friends, classmates, etc. You must complete the test using only your own knowledge and skills, and a writing instrument (pencil or pen).

Final Examinations Policy: All final exams are to be scheduled in accordance with the University's final examination policy.

X. Course Policies: Technology and Media

Email: For questions related to the course material, schedule, or grading, please first email the teaching assistant. If you have done so but are not satisfied with the response, please email the instructor. Allow at least 48 hours for a response.

Canvas: We will use Canvas to post grades and email any urgent announcements such as test-schedule changes. All course materials, including syllabus and an up-to-date schedule, are posted on the course webpage.

Usage of Phones and Other Devices: Besides taking notes (which is encouraged), please do not record class lectures in any way, including taking photographs or audio or video recordings.

XI. Course Policies: Student Expectations

Academic Integrity of Students: Academic integrity is the foundation of the University of South Florida System's commitment to the academic honesty and personal integrity of its university community. Academic integrity is grounded in certain fundamental values, which include honesty, respect, and fairness. Broadly defined, academic honesty is the completion of all academic endeavors and claims of scholarly knowledge as representative of one's own efforts. The final decision on an academic integrity violation and related academic sanction at any USF System institution shall affect and be applied to the academic status of the student throughout the USF System, unless otherwise determined by the independently accredited institution.

Students caught violating academic integrity, for example by using notes or a phone during a test, will receive an FF grade for the course.

Disruption to Academic Process: Disruptive students in the academic setting hinder the educational process. Disruption of the academic process is defined as the act, words, or general conduct of a student in a classroom or other academic environment which in the reasonable estimation of the instructor: (a) directs attention away from the academic matters at hand, such as noisy distractions, persistent, disrespectful or abusive interruption of lecture, exam, academic discussion, or general University operations, or (b) presents a danger to the health, safety, or well-being of self or other persons. USF's relevant policy is available at: http://regulationspolicies.usf.edu/regulations/pdfs/regulation-usf3.025.pdf

Student Academic Grievance Procedures: The purpose of these procedures is to provide all undergraduate and graduate students taking courses within the University of South Florida System an opportunity for objective review of facts and events pertinent to the cause of the academic grievance. An "academic grievance" is a claim that a specific academic decision or action that affects that student's academic record or status has violated published policies and procedures, or has been applied to the grievant in a manner different from that used for other students. USF's relevant policy is available at: http://ugs.usf.edu/policy/StudentAcademicGrievanceProcedures.pdf

Disability Access: Students with disabilities are responsible for registering with Students with Disabilities Services (SDS) in order to receive academic accommodations. SDS encourages students to notify instructors of accommodation needs at least 5 business days prior to needing the accommodation. A letter from SDS must accompany this request.

Sexual Misconduct/Sexual Harassment Reporting: USF is committed to providing an environment free from sex discrimination, including sexual harassment and sexual violence (USF System Policy 0-004). The USF Center for Victim Advocacy and Violence Prevention 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. This confidential resource can help you without having to report your situation to either 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 in compliance with Title IX and under the USF System Policy, 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. You may contact the USF Center for Victim Advocacy and Violence Prevention at 813-974-5757.

Campus Emergencies: 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, Elluminate, Skype, and email messaging and/or an alternate schedule. It is the responsibility of the student to monitor the Canvas site and emails for each class for course specific communication, and the main USF, college, and department websites, emails, and MoBull messages for important general information.

Attendance Policy: Students are expected to attend classes, but attendance is only directly taken on the first day of class. Again, the grading policy allows you to miss one test, due to illness or other emergency, without penalty.

Religious Observances: Students who anticipate the necessity of being absent from class due to the observation of a major religious observance must provide notice of the date(s) to the instructor, in writing, at the beginning of the term. If you observe religious holidays, you should plan your allowed absences to include those dates.

XII. ***Tentative*** **Schedule**

Week	Topics	Textbook Reading
1	Introduction; Definitions (policy, property, mechanism, enforcement, and CIA, safety, and liveness properties); Unenforceability of some policies	1.1-1.9
2	Threats; Tradeoffs; Secure software-design principles; **Test I**	2.1-3.9
3	Memory threats and mitigations, Part I: Access control as authentication and authorization; Role-based access control	Class notes
4	Memory threats and mitigations, Part II: Segmentation; Buffer overflows; StackGuard; ASLR; **Test II**	5.1-6.5
5	Memory threats and mitigations, Part III: Format-string and integer-overflow attacks; CFI; memory and control-flow safety with type-safe languages	6.6
6	Networking and communications; OSI layered architecture; client-server and peer-to-peer models; **Test III**	Class notes
7	Standard protocols (IP, UDP, TCP, HTTP); DoS; client-state manipulation	7.1-7.4
8	Firewalls; Intrusion-detection systems; **Test IV**	Class notes
9	Web clients, servers, and applications; Information management; Databases	Class notes
10	SQL queries and injection attacks; **Test V**	8.1
11	Parameterized queries; Stored procedures; Cross-domain security; XSS	8.2, 10.1-10.5
12	Symmetric cryptography; Block and stream ciphers; MACs; **Test VI**	12.1-3, 15.1-2
13	Asymmetric cryptography; Diffie-Hellman(-Merkle); RSA	13.1-13.7
14	Digital signatures; Key management; TLS; HTTPS; **Reading Day**	14.1-4, 15.3-5
15	**Test VII**; Password management; Review	9.1-9.6
Final	**Exam** (Monday, December 3, at 3-5pm)	(All tests are cumulative.)

This schedule is subject to adjustment as the semester progresses. The seven tests are scheduled to be held every fourth class meeting. Each test is expected to last 40 minutes. Although we will cover new material on test days, tests will only cover material from previous class meetings.