Secure Coding (CNT 4419)

CRN 95114, Section 001, 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 2019
Office Hours:	MW 2-3:30pm in ENB 333	Class Meeting Times:	MW 5-6:15pm
Course website	www.cse.usf.edu/~ligatti/sc/19/	Class Location:	CHE 101A
Teaching Assistant:	Kevin Dennis (kevindennis@mail.usf.edu)	TA Office Hours:	TTh 12-1:30pm in ENB 327

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 5 assignments, 6 tests, and 1 final exam. The lowest score on a non-final-exam test will be dropped, so final grades are determined by 5 assignment scores (each worth 2.5% of the final grade), the 5 highest 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+ (90,86.7], B (86.7,83.3], B- (83.3,80], C+ (80,76.7], C (76.7,73.3], C- (73.3,70], D+ (70,66.7], D (66.7,63.3], 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: No credit will be given for work turned in late. There are no make-ups or extensions for the assignments, 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, necessary travel, 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 tests and final exam 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 honesty: Everything you turn in for this class must be your own work. Students caught violating academic integrity, for example by using notes or a phone during a test, will receive an FF grade for the course.

Additional USF policies (e.g., regarding academic integrity) may be accessed at: https://www.usf.edu/provost/faculty/core-syllabus-policy-statements.aspx

XII. *Tentative* Schedule

Week	Topics	Textbook Reading
1	Introduction; Definitions (policy, mechanism, enforcement, property)	1.1-1.9
2	Definitions (safety, liveness, and CIA properties); Unenforceability	Class notes
3	**Test I**; Unenforceability	Class notes
4	Threats; **Test II**	2.1-2.9
5	Tradeoffs; Secure design; Access control; Authentication; Authorization	3.1-3.9, App. A
6	Memory segmentation; Buffer overflows; **Test III**	5.1-5.3, 6.1-6.5
7	StackGuard; ASLR; CFI; Type safety; Format string attacks	6.6
8	Format string attacks; Integer overflow attacks; **Test IV**	Class notes
9	Networking and communications; TCP/IP and OSI layered architectures; Protocols; DoS	Class notes
10	Firewalls; IDSs; Web applications; Client-state manipulation; **Test V**	7.1-7.4
11	OWASP Top 10; Databases; Information management; SQL queries	Class notes
12	SQL injection attacks	8.1-8.2
13	Code injections; XSS; **Test VI**	Class notes
14	XSS; Symmetric cryptography	Class notes
15	Asymmetric cryptography; Diffie-Hellman; RSA; Signatures; MACs; Password management	9.1-9.6
Final	**Exam** (Monday, December 9, at 3-5pm)	(All tests are cumulative.)

This schedule is subject to adjustment as the semester progresses. The six tests are scheduled to be held approximately every fourth class meeting (on 09/09, 09/18, 10/02, 10/16, 10/30, and 11/20). 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.