

**This syllabus was updated on 10/3/22. The only changes were to modify the test dates, due to Hurricane-related class cancellations on 9/26 and 9/28. All changes are highlighted.**

## Secure Coding (CNT 4419)

CRN 92721, 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 2022
Office Hours:	Online by appt., MW 2-3:30pm	Class Meeting Times:	MW 5-6:15pm
Course webpage:	<a href="http://www.cse.usf.edu/~ligatti/sc/22/">www.cse.usf.edu/~ligatti/sc/22/</a>	Class Location:	CHE 103
Teaching Assistant:	Kevin Dennis (kevindennis@usf.edu)	TA Office Hours:	Email for online appointment

☞ Everything on this syllabus is subject to change as the semester progresses.

#### 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 (1<sup>st</sup> 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 Required Readings

- Additional required online readings, if any, will be linked from the course webpage.

**VII. Basis for Final Grade**

There will be 4 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 4 assignment scores (each worth 2.5% of the final grade), the 5 highest test scores (each worth 12% of the final grade), and 1 final-exam score (worth 30% of the grade). All the tests and final exam are cumulative; earlier material may appear on any test or exam.

The scale for final letter grades is as follows, using standard notation for ranges: A ( $\infty$ ,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,- $\infty$ ). 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 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, work or family obligations, necessary travel, or an emergency.

*Because your lowest non-final-exam test score will be dropped automatically, do not email or otherwise notify the instructor or TA as to why, or even that, you're missing a test.*

**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.

**Essay Policy:** Tests and the final exam will often include one or more short-answer or essay questions. Respond in complete sentences. Avoid extraneous details in your responses. Responses 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 you'd like answered outside of class related to the course readings, 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. **The course schedule and assigned readings are posted on the course webpage.**

**XI. Course Policies: Student Expectations**

**Academic honesty:** Everything you turn in for this course 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.

**XII. USF Core Syllabus Policies**

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

**XIII. Tentative Schedule—subject to adjustment as the semester progresses—see the course webpage**

<u>Week</u>	<u>Topics</u>	
1	Introduction; Definitions (policy, mechanism, enforcement, property)	
2	Definitions (safety, liveness, and CIA properties); Unenforceability; <b>Test I</b>	
3	Unenforceability	
4	Threats; <b>Test II</b>	
5	Tradeoffs; Secure design; Access control; Authentication; Authorization	
6	Memory segmentation; Buffer overflows	
7	StackGuard; ASLR; CFI; Type safety; Format string attacks; <b>Test III</b>	
8	Format string attacks; Integer overflow attacks	
9	Networking and communications; TCP/IP and OSI layered architectures; Protocols; DoS; <b>Test IV</b>	
10	Firewalls; IDSs; Web applications; Client-state manipulation	
11	Databases; Information management; SQL queries; <b>Test V</b>	
12	SQL injection attacks	
13	Code injections; XSS; <b>Test VI</b>	
14	XSS; Symmetric cryptography	
15	Asymmetric cryptography; Diffie-Hellman; RSA; Signatures; MACs; Password management	
Final	<b>Exam</b> (Monday, December 5, at 3-5pm)	<i>*All tests and final exam are cumulative</i>

This schedule is subject to adjustment as the semester progresses. The six tests are scheduled to be held approximately every fourth class meeting (on 08/31, 09/14, 10/05, 10/19, 11/02, and 11/16). Each test is expected to last approximately 40 minutes. Although we will cover new material on test days, tests will only cover material from previous class meetings.