Secure Coding (CNT 4419)

CRN 86594, 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 2023
Office Hours:	Online by appt., MW 2-3:30pm	Class Meeting Times:	MW 5-6:15pm
Course webpage:	www.cse.usf.edu/~ligatti/sc/23/	Class Location:	CPR 115
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 (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 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, 3 tests, and 1 final exam. Each assignment score is worth 2.5% of the final grade, each test score is worth 20% of the final grade, and the final-exam score is 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 (∞,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.

Attendance: Attendance on non-test days does not directly affect final grades, but any absence may indirectly affect your final grade by putting you at risk of missing assignments, schedule updates, or material not covered in the textbook.

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-up tests, assignments, or final exam.*

Essay Policy: All tests and final exam will include one or more short-answer or essay questions. Respond in complete sentences. Avoid extraneous details in your responses. Also avoid using bulleted/enumerated lists in your responses. Responses will be graded based on readability, correctness, and thoroughness.

(Non-)Group Work Policy: Everything you turn in for this course—assignments, tests, and final exam—must be your own, individual work. All 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, assignments, 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 or copying another's student's solution, will receive an FF grade for the course.

Do not post your assignment solutions on any medium that could be accessed by other current or future Secure Coding students (e.g., in a public GitHub repository), as doing so may make you an accessory to another student's plagiarism.

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**

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

This schedule is subject to adjustment as the semester progresses. The tests are scheduled to be held approximately once a month, on 09/13, 10/11, and 11/08, and the final exam on 12/04. Each test is expected to last 75 minutes; the final exam is 2 hours.