Secure Coding (CNT 4419)

CRN 94124, 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 2021
Office Hours:	Online by appt., MW 2-3:30pm	Class Meeting Times:	MW 5-6:15pm
Course website	www.cse.usf.edu/~ligatti/sc/21/	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 (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 a 15-minute quiz at the end of every class meeting after the first week. Quizzes will cover material discussed in, and readings assigned for, *previous* class meetings. You won't be quizzed on readings that we discuss the same day as the quiz. *All quizzes are cumulative; earlier readings and class material may appear on any later quiz.*

Be sure to bring *blank* paper and a pen/pencil to each class, for taking the daily quiz. Please avoid using spiral bound paper for your quizzes.

There will also be 4 assignments, each worth 3% of the final grade. The remaining 88% of the final grade will be the average of the quiz scores—*after dropping the two lowest quiz scores*.

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. Quizzes will also be 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 or quizzes**. Because your two lowest quiz scores are dropped, you can miss two classes without penalty, for example due to illness, work or family obligations, or an emergency.

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

Essay Policy: Quizzes will often include one or more short-answer or short-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 quizzes in this course are closed books, notes, computers, phones, friends, classmates, etc. You must complete the quizzes using only your own knowledge and skills, blank paper, and a writing instrument (pencil or pen).

Final Examinations Policy: This course does not have a final exam.

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 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 quiz, 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. *VERY 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)
3	Unenforceability
4	Threats
5	Tradeoffs; Secure design; Access control; Authentication; Authorization
6	Memory segmentation; Buffer overflows
7	StackGuard; ASLR; CFI; Type safety; Format string attacks
8	Format string attacks; Integer overflow attacks
9	Networking and communications; TCP/IP and OSI layered architectures; Protocols; DoS
10	Firewalls; IDSs; Web applications; Client-state manipulation
11	OWASP Top 10; Databases; Information management; SQL queries
12	SQL injection attacks
13	Code injections; XSS
14	XSS; Symmetric cryptography
15	Asymmetric cryptography; Diffie-Hellman; RSA; Signatures; MACs; Password management