Secure Coding (CNT 4419)

CRN 94222, 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 2020
Office Hours:	Email for online appointment	Class Meeting Times:	MW 5-6:15pm
Course website	www.cse.usf.edu/~ligatti/sc/20/	Class Location:	CHE 103 (room cap=25)
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 will be linked from the course webpage.

VII. Online and In-person Class Meetings

For this course, you do not have to attend any class meetings in person. All the class meetings are accessible online. To do so, click the Blackboard Collaborate Ultra link in the Canvas page for this course and join the session.

Most of the class meetings will be driven by student questions or comments. When you want to respond to questions or enter the discussion while attending online, please use your judgment regarding whether to raise your hand in Blackboard Collaborate or simply unmute yourself and begin speaking. If too many people seem to be speaking at once, I will try to moderate the discussion and ask participants to raise their hands before joining the discussion. I apologize for mispronouncing your names when calling on you to speak.

This course will provide all students the opportunity to attend at least 21% of the class meetings in person (face to face). If you would like to attend in person, please email the TA and indicate how many class meetings you would like to attend in person. The TA will collect these emails, form a schedule for which students may attend on which days, and reply to you with the dates you may attend in person. This process exists because the course has more students enrolled than are allowed at one time in the classroom.

VIII. Basis for Final Grade

There will be a 15-minute quiz at the beginning of every class meeting after the first week. Final grades are determined by dropping the two lowest quiz scores and averaging the remaining quiz scores.

Quizzes will cover readings assigned for previous class meetings and material discussed in previous class meetings. You won’t be quizzed on readings that we haven’t yet had a chance to discuss in class. *All quizzes are cumulative; earlier readings and class material may appear on any later quiz.*

Each quiz will be posted on Canvas by 5pm and due at 5:15pm. To obtain credit for a quiz, you must upload your responses to the quiz problems as a single .txt or .pdf file in Canvas, or, if you run into technical problems uploading to Canvas, you may email your .txt or .pdf file to the TA, in which case the email timestamp will be used to determine time of submission. Please note that email timestamps may show later times than the actual times of sending (e.g., due to network delays), so to be safe please try to complete quizzes on time. You also can mitigate quiz issues by uploading drafts of your responses to Canvas during the quiz—you may submit quiz responses in Canvas as many times as you would like; we will grade your most recent submission. **If attending class in person, you must bring a computer on which to complete the daily quiz.**

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.

IX. Grade Dissemination

All grades will be posted on Canvas. Quizzes will also be discussed in class.

X. Course Policies: Grades

Late Work Policy: The hard deadline for submitting a quiz on time, for full credit, is always 5:15pm. Each quiz may be submitted up to 5 minutes late with a 10% penalty. No credit will be given for quizzes submitted after 5:20pm on the due date. **There are no make-ups or extensions for 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 typically 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 must be completed on your own, without assistance from anyone else. You may use static, non-human resources such as notes, research papers, the textbook, and existing Internet postings (e.g., Wikipedia articles) when completing quizzes. **However, you must not plagiarize any source—all of your short-answer and essay quiz responses must be written in your own words.**

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

XI. 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 quizzes, collect quiz responses, post grades, and email any urgent course announcements. We will also hold class meetings online through Blackboard Collaborate, accessible through Canvas. **The course schedule and assigned readings are posted on the course webpage**.

XII. Course Policies: Student Expectations

Academic honesty: Students caught violating academic integrity, for example by working together or receiving other human assistance during a quiz, will receive an FF grade for the course.

XIII. Standard University Policies

Policies about disability access, religious observances, academic grievances, academic integrity and misconduct, academic continuity, food insecurity, and sexual harassment are governed by a central set of policies that apply to all classes at USF. These may be accessed at: https://www.usf.edu/provost/faculty/core-syllabus-policy-statements.aspx Additional USF policies (e.g., regarding academic integrity) may be accessed at: https://www.usf.edu/provost/faculty/core-syllabus-policy-statements.aspx

XIV. Covid-19 Procedures

All students must comply with university policies and posted signs regarding COVID-19 mitigation measures, including wearing face coverings and maintaining social distancing during in-person classes. Failure to do so may result in dismissal from class, referral to the Office of Student Conduct and Ethical Development, and possible removal from campus.

Additional details are available on the University's Core Syllabus Policy Statements page: https://www.usf.edu/provost/faculty/core-syllabus-policy-statements.aspx

XV. *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); Unenforceability
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