General information

Section: 001, CRN: 25369, Credit hours: 3, Class meetings: MW 2-3:15pm in ENG 003
Instructor: Jay Ligatti (ligatti@cse.usf.edu)
Office hours: Online, by appointment, at TTh 10:30am-12pm

Course description: Introduction to research in foundations of software security. Basic static and dynamic enforcement of security policies. Roles and meanings of policies, properties, mechanisms, and enforcement. Language-based security and tools for specifying security. ***Student outcomes****:* Students having successfully completed this course will obtain a breadth of knowledge in the foundations of software security by reading a selection of research papers in the area and will obtain a depth of knowledge by performing independent research in the area.

Course materials

All readings will be from papers available online or handed out in class. Please check the course website (http://www.cse.usf.edu/~ligatti/foss/22) regularly for announcements, links to reading material, and an up-to-date schedule. Please attend each class with access to the paper we are discussing that day; our in-class discussions will often reference specific definitions and passages in the research papers. Grades will be posted on Canvas (http://my.usf.edu/).

Tentative schedule

Week	Dates	Topics
1	01/10, 01/12	Introduction and definitions; Research publications
2	01/19	Enforceability theory
3	01/24, 01/26	Enforceability theory
4	01/31, 02/02	Enforceability theory; Policy specification and composition
5	02/07, 02/09	Policy specification and visualization
6	02/14, 02/16	Firewalls; Authentication
7	02/21, 02/23	Authentication; IoT; Privacy; Cryptography
8	02/28, 03/02	Vulnerability trends; Buffer overflows
9	03/07, 03/09	Code and noncode injection attacks
10	03/21, 03/23	Student presentations (project proposals)
11	03/28, 03/30	CFI
12	04/04, 04/06	Memory (un)safety
13	04/11, 04/13	Hardware security
14	04/18, 04/20	Trustworthiness; backdoors
15	04/25, 04/27	Student presentations (final project presentations)

Final-grade breakdown:

- 50% Quiz average (after dropping 2 lowest quiz scores)
- 10% Peer reviews
- 10% Presentations (proposal presentation and final presentation are each 5%)
- 30% Research paper, due in class on April 27 at 2pm

Quizzes:
In every class meeting (except the first class and during student presentations), we'll have a quiz. Quizzes will:

- be closed notes, papers, books, phones, laptops, neighbors, etc.
- occur at the beginning of class.
- cover any reading for the current class meeting, as well any material discussed during previous class meetings.
- require you to write responses on paper to oral prompts. Bring *blank* paper and a pen/pencil to every class meeting, for the quiz. Do not use spiral-bound paper for quizzes.
- be graded on accuracy, thoroughness, and readability. Write in complete, easy-to-read, well-organized, English sentences. Avoid irrelevant details. Because quizzes are intended, in part, to evaluate and improve your skills at writing prose, avoid bulleted lists in your responses.

Quizzes will typically cover the following sorts of topics about the readings:

- What's the problem being addressed? (Motivation)
- Why don't existing approaches address that problem? (Related Work)
- How does the new solution work and go beyond prior work? (Contributions)
- What evidence exists, that the proposed solution works? (Experiments or Proofs)
- Where was the paper published? What quality of review exists at that venue?

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. I'll automatically drop your 2 lowest quiz scores, so please don't email me about absences.

Research project:
The centerpiece of this course is a research project. Students can work on the project alone or in small groups of 2 or 3 students. The project involves performing and presenting original research in the broad area of software security.

The research project is broken up into:

- A presentation for the class, given immediately after Spring Break, describing the problem you plan to work on, existing approaches to the problem, and techniques you're using to try to address the problem. The presentation will be graded based on peer and instructor evaluations.
- An in-class presentation of your research findings, at the end of the semester, graded based on instructor evaluation.
- A final research paper, due in hardcopy at the beginning of the final class meeting. Your paper should present original, but likely small-scale, research in the broad area of software security. This paper will be graded on readability, correctness, thoroughness, novelty, and significance. It is expected that your paper will be 4-7 pages in length, including well-formatted references.

Students will also be asked to review the project proposals of their classmates by emailing me, for every proposal presentation besides their own, exactly one paragraph describing the primary strengths and/or weaknesses of that proposal. Valid points made in peer reviews will help determine presentation grades.

Send peer reviews as plain text in the body of an email (not as an attachment). Reviews of proposal presentations are due at 5pm on 3/24.

Late submission:
The only graded items that can be turned in late for credit are peer reviews and final research papers. These items can be emailed up to two days late with a 15% penalty.

Attendance:
I do not take attendance directly, but quizzes and presentations are an indirect method of requiring attendance.

Grading system:
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]
F $(60,-\infty)$		

An A+ may be awarded for exceptionally outstanding work.

Additional, optional reading:
Some students may wish to supplement the papers being read this semester with more introductory readings from a textbook. If you're such a student, I'd recommend "Information Security: Principles and Practice" by Mark Stamp. Readings from this textbook are optional; I expect you'll learn what you need for this course just by (1) reading the assigned papers, (2) using web searches to figure out unfamiliar topics, (3) participating in our class discussions, and (4) doing your research project.

Academic honesty:
Academic honesty is crucial in research; cite sources and do not plagiarize. You'll receive an FF grade if you're caught cheating or plagiarizing in any way for this course.

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

Every part of this syllabus is subject to adjustment as the semester progresses. Please contact me as soon as possible if you're dissatisfied with the course policies, discussions, readings, grading, etc.; I'll be happy to accommodate reasonable requests for modifications.