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

General information

Section: 001, CRN: 18920, Credit hours: 3, Class meetings: MW 2:00-3:15pm online
Instructor: Jay Ligatti (ligatti@cse.usf.edu)
Office hours: Please email for an online appointment

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. Please check the course website (http://www.cse.usf.edu/~ligatti/foss/21) regularly for announcements, links to reading material, and an up-to-date schedule. You will also use Canvas (http://my.usf.edu/) to see course grades and attend class.

Attendance

To attend class, click the Blackboard Collaborate Ultra link in the Canvas page for this course and join the session.

Class meetings will be driven by a discussion of research papers, including questions and comments from students. As a student, when you want to enter the discussion, 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'll 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.

Please do not record class lectures in any way, including taking screenshots or audio or video recordings. This policy is intended to respect everyone's privacy and create an open atmosphere for dialog.

I will email any notes I type during class meetings, so you don't have to spend class time typing what I'm typing.

Final-grade breakdown

50%	In-class participation
50%	Research paper, due by 11:59pm on May 1

Class participation

Most class time will be spent reading and discussing research papers in the broad area of software-security foundations (i.e., theories, models, and philosophies underpinning software security).

The readings will be posted at http://www.cse.usf.edu/~ligatti/foss/21. Please attend each class online 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.

In all class meetings after the first, everyone is expected to participate nontrivially in the discussion. Participation may include asking or answering questions, or providing comments such as your opinions about the strengths or weaknesses of the research being discussed. You are expected to participate by speaking. If you have an accessibility issue that prevents or hinders your ability to participate by speaking, please let me know before the next class meeting, so we can work out an alternative.

Participation will be scored for each class meeting after the first using a scale of 0-10, where 0 indicates no participation (including due to an absence) and 10 indicates participation by asking an interesting question or making an interesting comment (i.e., a question or comment that's interesting to me or seems like it could be interesting to the other students). Any nontrivial, understandable participation will receive at least a 6.

Research paper: The other half of your grade is determined by a research paper due on May 1. You may write this paper alone or with another student enrolled in this course. 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 would be 4-7 pages in length, including well-formatted references. Submit your paper by emailing it to me (ligatti@usf.edu) by 11:59pm on May 1.

Late submission: No credit will be given for any coursework submitted late.

Grading system: 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.

Academic honesty: Students caught violating academic integrity, for example by plagiarizing in a research paper, will receive an FF grade for the course.

Many additional USF policies (e.g., regarding academic integrity and COVID-19) may be accessed at: https://www.usf.edu/provost/faculty/core-syllabus-policy-statements.aspx

Tentative schedule

Week	Dates	Topics
1	01/11, 01/13	Introduction and definitions; enforceability theory
2	01/20	Enforceability theory
3	01/25, 01/27	Enforceability theory
4	02/01, 02/03	Enforceability theory; Policy specification and composition
5	02/08, 02/10	Policy specification and visualization
6	02/15, 02/17	Firewalls
7	02/22, 02/24	Authentication
8	03/01, 03/03	Vulnerability trends; Buffer overflows
9	03/08, 03/10	Code and noncode injection attacks
10	03/15, 03/17	Injection attacks
11	03/22, 03/24	CFI
12	03/29, 03/31	CFI
13	04/05, 04/07	Noninterference and information flow
14	04/19, 04/21	Usable security; DRM
15	04/26, 04/28	Trustworthiness; backdoors