General Information

Class meetings: TTh 5-6:15pm in BSN 1403
Professor: Jay Ligatti (ligatti@cse.usf.edu)
Office location: ENB 333
Office hours: TTh 3:30-5pm, and other times by appointment

Course objectives: 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 policies.

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-16) regularly for announcements, links to reading material, and an up-to-date schedule. Grades will be posted on Canvas (http://my.usf.edu/). I may also send announcements via Canvas, so please ensure that your current email address is stored in Canvas.

Tentative Schedule

Week	Dates	Topics
1	01/12, 01/14	Introduction and definitions; enforceability theory
2	01/19, 01/21	Enforceability theory
3	01/26, 01/28	Enforceability theory
4	02/02, 02/04	Enforceability theory
5	02/09, 02/11	Policy-specification languages
6	02/16, 02/18	Policy-specification languages; Stack inspection
7	02/23, 02/25	Vulnerability trends; Buffer overflows
8	03/01, 03/03	Code-injection attacks
9	03/08, 03/10	Web security; XSS
		[Spring "break"]
10	03/22, 03/24	Student presentations (project proposals)
11	03/29, 03/31	CFI; Noninterference and information flow
12	04/05, 04/07	Physical security
13	04/12, 04/14	DRM
14	04/19, 04/21	Trustworthiness; backdoors
15	04/26	Student presentations (final project presentations)

Final-grade breakdown:

40%	Quiz average
10%	Peer-proposal reviews
10%	Research project: Proposal presentation
7%	Research project: Final presentation
33%	Research project: Final research paper, due in class 4/26

Quizzes:
In every class meeting (except 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, and
- require you to write responses on paper to oral prompts. Quizzes will be graded, in part, on how well your ideas are communicated. Please write as you would in a research paper, with easy-to-read, grammatically correct English sentences.

Please bring paper and a pen/pencil to every class meeting, for the quiz.

Your 2 lowest quiz scores will be dropped. This policy enables you to miss class for a week due to an emergency or illness, without it affecting your grade. 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, again graded based on peer and instructor evaluation.
- *Optional*: A rough draft of a research paper, as long as it's given to me in class by 4/19. I'll comment on all the issues I see in a rough draft, so you'll know what to focus on improving.
- A final research paper, due in the final class meeting on 4/26, graded based on readability, novelty, and significance.

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 3/26.

Late submission:
There are no makeup quizzes in this course. 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 are an indirect method of requiring attendance. Students who will miss class for religious reasons must notify me of the date(s) in writing by the end of the first week of classes. Please do not sell notes from, or record, class meetings without my permission.

Grading system:
For final letter grades, I'll use the standard scale of A (100-90%), B (89-80%), C (79-70%), D (69-60%), and F (59-0%). I'll also use pluses and minuses on final grades to indicate either a borderline grade (i.e., within 2.5 points of an adjacent grade) or exceptionally outstanding work (A+).

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 entirely optional; I'm not expecting you to do them. I expect you'll learn what you need for this course just by (1) reading the assigned papers, (2) using Internet 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.

Of course, 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.