Software Security

Bulletin Description

This is a graduate course in software security. We will learn about various security policies across a range of application domains and we will evaluate the tools and techniques used to enforce those policies. Classes will be organized around paper reading and a final project.

General Course Info

Term:	Spring 2018
Department:	COMP
Course Number:	790
Section Number:	132
Time:	TTh 2:00 – 3:15
Location:	FB 008
Website:	http://cs.unc.edu/~csturton/courses/swsec/790-132-sp18.html

Instructor Info

Name:	Cynthia Sturton
Office:	FB354
Email:	csturton@cs.unc.edu
Phone:	919-590-6020
Website:	http://www.cs.unc.edu/~csturton
Office Hours:	By appointment

Textbook and Resources

There are no required textbooks. Required readings will be posted online in the course schedule.

Course Description

A secure system is one that will enforce a given policy, even in the face of malicious activity.

In this class we will learn about different security policies and how they apply across a variety of application domains. We will read about mechanisms designed to enforce a given policy and attacks meant to thwart that same policy.

Target Audience

The class is meant for students who are interested in software and systems security. The course will be research focused: classes will be centered around discussion of published research in the security community, students will work on an original research project, and students will write a conference-style paper describing their work.

Prerequisites

This class is open to all CS graduate students. Undergraduate CS students and graduate students outside the CS department who wish to take the class should attend the first lecture and speak to the instructor at the end of class.

Course Requirements

Students will read 1 to 2 papers per class. Classes will be organized around a combination of lecture and paper discussions; reading the paper is necessary in order to contribute to the discussion. For each paper, students will write a short synopsis and review.

Each student will be responsible for presenting 2–3 papers over the course of the semester.

Students will work in groups of 2 on an original research project. At the end of the semester, each group will submit a conference-style paper and give a short (10–15 min) presentation in class describing their work.

Key Dates

Project proposals due: 2/15/18
Final in-class presentations: 4/24/18, 4/26/18
Final project report due: 4/28/18

Grading Criteria

Final project: 50%
Class discussion & written reviews: 20%
Paper presentations: 30%

Course Policies

Classes are centered around discussions of papers; attendance is necessary in order to participate in the discussion.

Honor Code

Discussion of the assigned papers outside of the classroom is encouraged; however, collaboration on the written paper reviews is not permitted. Any outside source used as part of a paper review (other papers, textbooks, websites) must be properly cited.

Collaboration with one other student is allowed for one of the security reviews. The other security review must be done individually. If you are collaborating with another student, you may submit a single write-up. Be sure to include the names of both students on the submission. Any outside source used as part of a security review (other papers, textbooks, websites) must be properly cited.

The final project must be original research. Students will work in groups of 2 or 3 for the final project, and submit one written report per group.

In the course of this class we may discuss known vulnerabilities and attacks on computer systems. This is not an invitation to exploit these vulnerabilities in real systems. You may not attempt to break into any system that is not your own; you may not attempt to thwart or circumvent the security of any system that is not your own. Doing so is, at a minimum, a violation of the honor code.

Course Schedule

The course schedule will be posted on the course website.

Disclaimer

The professor reserves to right to make changes to the syllabus, including project due dates. These changes will be announced as early as possible.