

Computer Security Concepts

Bulletin Description

This course provides an introduction to topics in computer security. We will cover a breadth of topics including confidentiality, integrity, availability, and authentication policies, basic cryptography and cryptographic tools, concepts in software security and network security, and legal and ethical considerations for security. The course will incorporate discussion of topical events in the news.

General Course Information

Term: Fall 2019
Department: COMP
Course Number: 435
Section Number: 001
Time: MW 3:35-4:50
Location: Genome Sciences G200
Website: <https://cs.unc.edu/~csturton/courses/securityconcepts/435-fa19.html>
Piazza: <https://piazza.com/unc/fall2019/comp435>
Gradescope: <https://www.gradescope.com/courses/46473>

Instructor Information

Name: Cynthia Sturton
Office: FB354
Office Hours: Fridays 2-4
Email: 435f19instructors@cs.unc.edu
csturton@cs.unc.edu
Website: <http://www.cs.unc.edu/~csturton>

Teaching Assistants & Learning Assistants

TAs: Dylan Tastet
Saumya Ray
Perry Healy
LAs: Kimia Pourali
Bokai Li
Email: 435f19instructors@cs.unc.edu

Resources & Textbook

The required textbook is Security in Computing, 5th Edition by Pfleeger, Pfleeger, and Margulies
ISBN: 9780134085043 Publisher: Prentice Hall

The course schedule, announcements, and reading assignments will be posted on the class website.

The class Piazza site is the best place for you to ask your questions. Here are some guidelines.

- If you are wondering about something, ask a question!
- Answer other students' questions and refine existing answers.
- Be polite; be kind.
- Do not post code or ask others to post code.
- You may post privately to the instructors, but we reserve the right to make all or part of the post public if we feel the question is of general interest to the class. (If we do this, we won't reveal any personal information about the original poster.)
- We may post questions on Piazza that get emailed to the instructors if we feel the question is of general interest to the class.

Course Description

Building secure systems is the responsibility of all computer scientists, not just a few security specialists. To that end, this class will foster in students a security mindset—a way of examining any system to find vulnerabilities and assess their effect on security. Along the way, students will learn about the types of security policies one might care about, how attackers can and have thwarted security, sometimes in surprising ways, and what steps computer scientists and engineers can take to improve the security of their own systems. The course will cover aspects of security ethics and privacy and will incorporate discussion of related events in the news.

Target Audience

This class is meant for computer science students who wish to develop literacy in foundational computer security topics. Students who have already taken Introduction to Computer Security (COMP535) should not enroll in this class.

Prerequisites

The prerequisites are COMP 410 and COMP 411.

Goals and Key Learning Objectives

By the end of the course students will be able to:

- Apply a “security mindset” across major application domains
- Explain the basic building blocks of security
- Evaluate a given security policy in one of the major application domains
- Assess the support for security in a given system
- Create and apply a strategy for teaching oneself about a new technical domain
- Distinguish privacy as a consideration different from security
- Analyze basic legal terms regarding intellectual property

Course Requirements

Classes will be organized around lectures, discussion, and in-class exercises. There will be assigned readings from the textbook as well as additional readings that will be posted on the class website. There will be five to six assignments over the course of the semester, one presentation, one midterm, and a final exam.

Key Dates

Midterm exam: 10/09/2019 (tentative)
Final exam: 12/07/2019 4–7 P.M.

Grading Criteria

Assignments: 50%
Project: 15%
Midterm exam: 15%
Final exam: 20%

Course Policies

No laptops or mobile devices in the classroom.

Assignments will be submitted electronically. Late assignments will lose a third of a letter grade (A becomes A-, A- becomes B+, etc.) every 24 hours. In other words, assignments turned in within the first 24 hours after the deadline will lose one third of a grade; assignments turned in between 24 and 48 hours after the deadline will lose two thirds of a grade, and so forth.

The course final is given in compliance with UNC final exam regulations and according to the UNC Final Exam calendar.

Honor Code

Assignments are to be done individually. Students may discuss the assignment with others, but may not share code.

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 and likely a violation of the law. Use caution; even accidental exploits may be subject to prosecution.

Course Schedule

The course schedule will be posted on the course website.

Disclaimer

The professor reserves the right to make changes to the syllabus, including exam dates. These changes will be announced and posted on the class website as early as possible.