COMP 535: Introduction to Computer Security

Bulletin Description

Principles of securing the creation, storage, and transmission of data and ensuring its integrity, confidentiality, and availability. Topics include access control, cryptography and cryptographic protocols, network security, and online privacy.

General Course Info

Term: Fall 2016  
Department: COMP  
Course Number: 535  
Section Number: 001

Time: 1:25 – 2:40pm on MW indicated on the web page  
Location: FB007  
Website: http://www.cs.unc.edu/~reiter/fall2016/

Instructor Info

Name: Prof. Michael Reiter  
Office: FB350  
Email: reiter@cs.unc.edu  
Web: http://www.cs.unc.edu/~reiter  
Office Hours: 10-11am on most Fridays (check course web page)

Teaching Assistant

Name: Ke (Coby) Wang  
Email: kwang@cs.unc.edu  
Office Hours: 3-4pm on Mondays and 1-2pm on Tuesdays  
Location: FB352

Textbooks and Resources

There is no textbook for this class. The class lectures will be posted before class (usually), and some readings will be assigned. There are no plans to use Sakai.

Course Description

The goal of this course is to explain the principles behind computer security threats and countermeasures seen today or emerging soon. In particular, we will place an emphasis on principles and, where possible, rigor. Developing
exploits will not be a focus of the class, though some assignments will involve implementing some attack code.

Target Audience

The target audience for this class is computer science students, especially those planning to go on to software architect/developer jobs in industry or to pursue graduate studies.

This class may be useful for system administrators, but you will not learn about specific products or how to configure them.

Prerequisites

COMP 410 and MATH 381. Some other skills that would be useful are a basic understanding of probability; exposure to basic networking concepts; and some familiarity with the C and Java programming languages.

Goals and Key Learning Objectives (subject to change)

Through this course, students will accumulate familiarity with the following technologies: access control and authentication in distributed systems; cryptography and cryptographic protocols (mainly key exchange protocols); user authentication; software vulnerabilities and software engineering to reduce vulnerabilities; firewalls and related technologies; network denial-of-service and defenses; technologies to support online privacy; and selected advanced topics (time permitting).

Course Requirements

The nature of work in this class is primarily in working problems presented through quizzes and exams, and in solving a few programming assignments.

Key Dates

Exam dates and assignment due dates are unknown at this time and will be announced as soon as they are known. I plan to have a brief quiz once per week.

Grading Criteria (subject to change, but roughly the following)

20% Weekly quizzes
40% Programming assignments (probably 3-4 during the semester)
20% Midterm exam
20% Final exam
Course Policies

Class attendance, per se, is not evaluated. However, since there will be regular class quizzes, missing classes means missing quizzes; each missed in-class quiz, regardless of the reason for missing, receives a score of zero, and making up quizzes is not permitted. Each person will be permitted to drop their lowest two quiz grades, however.

Late assignments will not be accepted unless otherwise stipulated.

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

Honor Code

The degree of collaboration permitted and the resources that should be used will be specified per assignment. However, the default policy is that no collaboration or resources except those specifically provided as part of the class (e.g., class notes and recommended readings) should be used in completing assignments. All work must be your own.

Course Schedule

The course schedule is posted at the course web page and will be updated often. Please check it frequently.

Disclaimer

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