CS-451: Computer Security

Calvin Deutschbein (they)

Willamette University, Fall 2021

E-mail: ckdeutschbein@willamette.edu
Office Hours: By Appt. & TBA
Office: Zoom, Ford 206

Web: **cd-public.github.io/**
Lecture MWF 11:30-12:30
Lecture Hall: Ford 204

Course Description

Cybersecurity can be understood as a mindset or approach rather than a subfield of computer science, such as secure mobile computing, network and operating system security, secure data bases, and secure cryptography algorithms. This course prepares a general computer science audience familiar with writing and understanding code to incorporate security concepts and ethics into the systems they develop or manage.

Required Materials

Required materials will be available on the course webpage under resources.

Prerequisites

This class is meant for computer science students who have completed introductory coursework in programming. Students should complete CS 141/151 and CS 241 before enrolling in this class.

Accessability

I will make every effort to ensure all coursework and materials are accessible to all students, including working with on-campus specialists. However, there is always room for improvement. I always appreciate hearing from students about how I can make the course more accessible, so please reach out if there is something I can be doing better!

Course Objectives

This course will teach you techniques for reasoning about information and computing and controlled accesses to these resources. As a survey course of the broad discipline of computer security, it will focus on different abstraction levels, from cryptographic code at a low level to the cultural and economic implications of secure and insecure data access at a high level.

- You will practice styles of thinking used by security researchers to contextualize their work in the broader context of computing and society.
- You will gain experience working with common coding practices for security, especially in the context of network and internet security.
- You will learn some historical efforts to attack and defend various computing systems, and discuss the implications of the state of computer security as a discipline and as deployed in practice..
- You will learn some theoretical background in formulating notions of security (the "logical foundations" of computer security).
- You will be exposed to state-of-the-art security research specific to hardware designs, including computer processors, as an example of ongoing research efforts.

This course will equip you apply notions of computer security to your other coursework, within computer science as well as within the college, and empower you to be a responsible computer scientist and member of an increasingly computer reliant society.

Course Structure

The course will be composed of lectures, labs, homeworks, midterms, and a final project.

Class Structure

Lectures are scheduled for Mondays, Wednesdays, and Fridays at 11:30 AM in Ford 204. The schedule of lectures will be available on the course webpage under schedule.

The course will be composed of two parts. In the first part of the course, class will be used for lecture on low level security concepts. In the second part of the course, class will be used for discussion of high level implications of computer security.

Lectures will be a combination of white board work and demonstrations. I will support a remote option for all lectures, likely through a streaming platform or Zoom, and will post recordings of lectures on the course website. While I will make every effort to follow best practices for accessible teaching, I will make mistakes! Please, if you find some material is inaccessible for any reason do not hesitate to reach out.

Discussions will be conducted in a format to be agreed upon by the class, whether in person, hybrid, or Zoom. Participation in lecture will be required and will be considered in course grades, both during class and in advance.

Homework Structure

Feedback will be provided on homework assignments. Homework assignments will be considered when determining grades for this course.

Homeworks will consist of programming assignments to be completed outside of class and submitted for feedback. There will be a "Homework 0" at the beginning of the semester to get used to programming and assignment submission, then two homework assignments throughout the semester. You will always have at least two weeks to complete homework assignments.

Homework assignment will be due at 11:30 AM on Fridays so we can discuss them in class on the day they are due.

As a rule, I encourage students to submit their assignment as-is at the due date and not to submit late work. By way of explanation, it is my experience as both a student and a grader that time spent working on assignments after their deadline is often better spent working on the next assignment.

As-is submission is supported in the grading policy by dropping the lowest homework grade. In special circumstances such as extended medical problems or other unforeseeable emergencies, please reach out and so we can collaboratively develop a more personal solution to achieve the learning objectives of the course.

Midterm Structure

Feedback will be provided on midterm exams. Midterm exams will be considered when determining grades for this course.

There will be two written midterm final exams, intended to be completed individual without access to notes or documentation. The midterms are intended to achieve a learning focus of reasoning about data structures in isolation from coding environments, as well provide me as an instructor with greater insight into how effective course instruction has been.

Discussion Participation

Discussion participation will be considered when determining grades for this course.

Discussion participation will be intermediate between homework assignments and discussion class sessions. Discussion class will be driven by reviewing primary or secondary source documents relevant to some prominent case of a security breech of secure systems. Students will be expected to review these materials prior to class, and a submit a 1 or 2 paragraph reflection on the reading no latter than midnight before class, to be submitted by email (to give me time to read them before moderating discussion).

If you will be unable to attend class for any reason, be submit a reflection prior to the deadline and not you will not be able to attend.

Beginning the week of November 1, topics and readings will be chosen by a student and discussion will be moderated by that student. A list of potential topics will be provided, or students may chose their own topic in consultation with the instructor.

Final Project

Feedback will be provided on the final project. The final project will be considered when determining grades for this course.

There will be a final project that will be similar in format but distinct in content from discussions. Final projects are intended to be undertaken collaboratively with other students and provide a detailed overview of an important topics in computer security and society. Projects will be presented beginning the week of November 29 after submitting a project proposal by (Friday) October 29.

Feedback and Grading

Feedback will be provided on assignments, midterms, and the final project using a 100 point scale. Discussions will be graded by participation. This 100 point scale is intended to be familiar to established grading standards, such as letter grades. To provide aggregate feedback for the whole course, these feedback scores will be combined as follows:

- **20%** of your grade will be determined by homework assignments

  10% each for the two highest scored assignments (out of three).

- **40%** of your grade will be determined by midterm exams.

  20% each for the two midterms.

- **20%** of your grade will be determined by discussion participation.

  10% each for leading a discussion and participating in other discussions.

- **20%** of your grade will be determined by the final project.

Feedback scores will constitute the minimum grade on an assignment, but the instructor may exercise discretion at any time to award a higher grade. For example, a submitted homework may not use some important algorithmic technique as submitted, but if the student showed familiarity with this technique on an earlier assignment or exam, the absence of that technique in a specific case need not be counted against a student in grading, but only noted in feedback. This corresponds to the high level notion of feedback corresponding to how well an assignment reached the intended learning goals, while the overall course grade is meant to indicate that a student is prepared to succeed in latter coursework. Under this model, the final project will offer an opportunity to show familiarity with all content in the course, so a strong final project can ensure a high course grade for any student, regardless of prior scores on midterms and homeworks.