CS 28 — NETWORKS AND CRYPTOGRAPHY
COURSE INFORMATION

Be sure to read all of this document!

1 Description

1.1 Networks

Computers are useful devices in isolation, but when you connect them, a wide variety of new uses emerge. We have become accustomed to networked computers (thanks to the Internet, cheap ethernet, and nearly ubiquitous WiFi hotspots), but (by design) it is not obvious to the user **how** the data gets from one machine to another. The first concern of this course is to examine the problems that must be solved in order to perform computer communication, and then the interesting problems that arise once they are connected.

Computer networks are commonly viewed as a group of *layers*. At the bottom-most layer is the simple capability of sending a signal through a wire (or through space, in the case of radio waves). Once that capability is established, though, there must be a convention to determine what the signals **mean**. Then you must be certain that the signals received are **correct**. Then you connect more than two computers together, and you have to coordinate which one gets to send a message at what time. Connect enough computers together, and then you must figure out how each computer can **find** the other to send it a message. We will address these questions (and more) by examining the following layers:

- Physical (wires and signals)
- Data link (flow control, errors, protocols)
- Medium access (coordination and collision)
- Network (routing and the Internet Protocol)
- Transport (sockets and TCP)

1.2 Cryptography

Given the ability of computers to communicate, users will transmit all manner of information through computer networks: from the mundane to the critical, data that is sensitive for individuals, institutions, businesses, governments, and military. It is important not only that information be communicated, but that it be *secure*—that a sender can be certain that it can be read only by those parties for whom it is intended. Each receipient must also be able to verify both that the data came from the claimed sender, **and** that the data has not been modified in transit.

Cryptography is the study both of methods of *encryption* and of *cryptanalysis*—the techniques used to *break* encrypted data, allowing someone to read data even without being the intended recipient. In this course we will examine the progression of cryptography over the ages. It began long before computational devices, but it has advanced dramatically since their inception. We will see how each approach to encrypt was developed, and we will examine cryptanalysis methods that broke existing codes and forced encryption techniques to advance. We will also see how modern encryption methods not only secure data, but also allow a recipient to verify the integrity of the data and the identity of its sender.

1.3 Security

There is more to securing your data than good encryption techniques—your encryption will not protect your data if someone else can intercept what you type on the keyboard as you enter your password. Computer systems and networks were originally designed to perform their tasks, with little concern for how they might be misused. A secure system must not only perform its intended task, but it must also prevent the use of the system for things other than its intended task. Since computers and networks are such general purpose devices, it is difficult to design systems that are both capable but also secure.

We will examine typical problems with creating secure software and communications. Controlling access is difficult, and preventing attacks that allow a user unauthorized or falsely authenticated access to a computer system requires a deep understanding of how those systems work. Through case studies, we will see how systems have been compromised in many ways, and then examine the techniques for preventing those attacks.

2 Lectures and labs

This class meets on **Monday, Wednesday, and Friday** of each week, from **9:00 am to 9:50 am**, in **Seeley Mudd 202**. You are expected to be present for **all of the lectures**, and so missing either is strongly discouraged. I will not teach material twice, so if you miss a lecture, you're on your own. If you must miss lecture due to an illness or other emergency situation, contact me and we will arrange to handle the situation. **If you have a conflict** with a lecture—for an athletic event, performance, or other extra-curricular activity, or to depart early for or arrive late from a vacation, or any other non-emergency—then **the choice is yours to miss or to attend**. If you choose to miss the class meeting, I do **not** want to know *why* nor even *that* you are missing class. You have elected, voluntarily, not to attend, and you must be prepared to obtain and learn the material that you missed on your own. I, of course, recommend that you choose to attend the class meeting when these conflicts arise. Do not underestimate the willingness of those who run extra-curricular programs to make accommodations for your academic demands.

I expect you not only to attend lectures, but also to be attentive for them. The time will be best spent if it is interactive, and that requires that you be up-to-date on the class material, and that you be alert and prepared to participate.

3 Texts and materials

The text for this course is *Computer Networks, 4/e*, by Andrew Tannenbaum, ISBN #978-0130661029. I have not ordered these texts at a local bookstore—you should be able to find copies without much trouble.

Any other materials for the course will be posted on the documents section of the course web pages.

4 Assignments, deadlines, and extensions

There will be a number of projects, and perhaps a problem set or two. The deadline for each will be stated clearly on the assignment, **down to the minute**. The assignment will also state the manner in which you are expected to submit or show your work. **Late submissions will receive failing grades**. Futhermore, **failure to complete any *one* of the labs or projects *may* result in a failing grade for the course**. These assignments are too important to the course not to be completed.

An extension for any assignment **must be requested, in writing** (email counts as *writing*), **at least 48 hours prior to the deadline**. The determination as to whether or not a particular situation merits an extension will be made on a case-by-case basis. Scheduled events are **not** sufficient reason to warrant an extension. Rather, extensions are intended for unusual circumstances that prevent you from planning your time well in order to meet the deadline. Note that a sudden onset of illness or other emergency situation that occurs less than 48 hours before a deadline will be treated as a special case.

5 Exams

There will be **one exam** in this course, the final exam, and it will be **an oral examination**. That is, each of you will schedule a one-hour time during reading or exam period, and during this time, you will be given questions for which you must present the answers in an interactive setting with me.

6 Grading

Your final grade will be determined by a formula roughly like the one below:

- 60% labs/projects
- 40% final exam

7 Academic dishonesty

You will be expected to do your own work on all assignments and exams in this course except where explicitly noted on group assignments. While I encourage you to interact with your classmates and discuss the material and assignments, there is a limit to the specificity of such discussions. I seek to make that limit clear here.

It is acceptable to discuss any assignment for the class with a classmate. You may even discuss your approach to a particular problem, or review relevant material for a problem with another person. However, you **may not show another student your work, nor see another student's work. If in doubt, *ask me***. If you are unsure whether or not a particular kind of communication would rise to the level of academic dishonesty, then you should contact me immediately and find out.