CMPS 122: Computer Security

Computer Science Department
University of California, Santa Cruz

Fall 2015

Time: MWF 9:30–10:40 AM
Location: Baskin Engineering 169
Instructor: Professor Ethan Miller (office: Engineering 2 365, elm@ucsc)
Office hours: Wed 3:00–4:00 PM; Fri 11:00 AM–noon
TA: Thomas Schmitz (office: Engineering 2 480, tschmitz@ucsc)
Office hours: Tue 4:00–5:00 PM; Wed 12:30–1:30 PM; Thu 3:00–4:00 PM
Prerequisites: CMPS 111
Optional texts: Carry On: Sound Advice from Schneier on Security, Schneier
Home page: http://classes.soe.ucsc.edu/classes/cmps122/Fall15/

Course objectives

The goal for students in this course is to learn the fundamentals of computer security, including:

• Principles of computer security
• Basic cryptography
• Authentication
• Secure network protocols (Kerberos, SSL)
• Attacks and defenses on computer systems
  • Firewalls
  • Intrusion detection
  • Countermeasures
• Program security
  • Bug exploits
  • Malicious code: viruses, worms, trojan horses, and more
• Database security
• Trusted operating systems
• Societal issues in computer security: legal, ethical, governmental

Additional topics may be covered, depending on the interests of the students and the professor. Where possible and appropriate, we’ll use examples from Linux, FreeBSD, and other modern operating systems as well as current events to illustrate concepts covered in class.
Prerequisites

The formal prerequisite for this course is CMPS 111 (Introduction to Operating Systems) before this class. Students who have not taken CMPS 111, but have a strong background in understanding computer systems, may be given permission to enroll—please contact the instructor. Students should also be familiar with basic probability and statistics, and knowledge of network protocols, though not required, is also helpful.

Readings

The required text is Computer Security, 3rd Edition, by Stallings and Brown. Most of the readings will be assigned from this book; lectures and class discussions will assume that you’ve read the material before the class. I didn’t ask the campus bookstore to stock the book, but you can get a copy online (e.g., from Amazon).

Ross Anderson’s excellent book Security Engineering is also helpful; you can download PDF of chapters from Anderson’s web page. I also recommend that you read Carry On: Sound Advice from Schneier on Security, a mostly non-technical book, because it provides short essays that provide context for many of the issues in computer security that we’ll explore in more depth in class.

Web pages

Most of the information for the class will be distributed via the Internet, available from either the course Web page or eCommons. We’ll be using Piazza for discussions. Much of the content on the class web pages is available only to users in the ucscl.edu domain, but you can use the off-campus access proxy or VPN to access these pages from off-campus.

Assignments, Exams, and Grading

Exams

There will be an in-class midterm around the first week of November and a final exam during the scheduled slot in exam week (Monday, December 7th from 4:00–7:00 PM). You must attend each exam at the scheduled time unless you are ill or have a death in the family. You must let the professor know by email or text message before the exam’s scheduled start regardless of the reason, and you must provide a doctor’s note or letter from the funeral home before you can make up the exam. There are no exceptions to this policy.

Homework assignments

There will be 5–6 homework assignments, one every week or two, assigned over the course of the quarter. The assignments may require some programming, which (unless otherwise specified) may be done in any programming language you want. Homeworks will be graded, and will be returned as soon as possible, typically within 7–10 days. Assignments will be posted on the SOE site. Due dates for all assignments will be listed on the class schedule, as well as on the assignment itself.

Homework must be kept in a git repository and submitted by committing your files and pushing them. We will grade the last version of your repository committed before the due date. Homework may be submitted from anywhere with an Internet connection; having a minor illness that keeps you home for a few days is not a valid reason for an extension. Since unexpected events do crop up, however, each student in the class may extend the due date of a single assignment during the quarter by up to 48 hours with no penalty and no excuse needed. To avail yourself of this opportunity, commit a file extension.txt in the assignment directory.

In addition to homework assignments, there are challenge problems—questions that may or may not have a solution. Solving a challenge problem gets you extra points, depending on how many people work on the solution.
Typically, only the first person to solve the challenge problem gets credit, though details may vary depending on the problem. More details on challenge problems are available from the course Web pages.

**Term project**

There is a required term project on a topic related to computer security. The project may be a programming project or a survey of papers on a particular area of computer security. There will be checkpoints throughout the quarter to ensure that you are making progress on your project. Checkpoints will not be graded separately, though your overall report will be graded. Your term project must turned in by the due date.

**Grades**

Your grades will be determined as follows:

- Homework: 35% (all assignments weighted equally)
- Project: 15%
- Exams: 45% (14% midterm, 31% final)
- Class participation: 5%

You must take both exams and turn in a final project to pass the class. You need not turn in every homework, but a missing homework counts as a zero (0). If your homework or exam average is below 50%, you will fail the class regardless of your overall average. Assignment grades will be available online in eCommons during the quarter.

**Attendance**

You’re expected to attend every class, though attendance won’t be taken, except as needed for UCSC administration. Much of the course material, including assignments and lecture notes, will be posted on the class web pages. However, things may get said in class that aren’t in the online notes. *You’re responsible for all material covered in class*, whether or not it appeared on the Web site—I suggest you ask either a fellow student or the professor or TA (in office hours, not via email) to fill in any material you may have missed.

**Getting help**

You’re strongly encouraged to seek help if you need it. You can do this by going to office hours, reading the Piazza forums, or by email. Office hours are optional, but highly recommended if you’re having any difficulty understanding the material, doing the homework assignments, or working on the term project. More in-depth discussions of security-related topics are also appropriate (and encouraged) during office hours. As a further incentive, I’ll have free espresso available in my office during office hours. You’re welcome to use the course forum and send email at any time, but please arrange any meetings outside of office hours in advance.

We’ll be using the Piazza forum for online discussions of material relevant to the course. I strongly encourage you to read the forum and post if you have general questions. Asking things like “how does this concept work?” or “what does this algorithm do?” are fine. Questions such as “what’s the answer to Problem 3 for this week’s homework?” are not acceptable. Please ask such questions during office hours. If you have questions about the grading of your assignment, they must be asked by email, not on the course forum. Of course, generic questions about assignments or grading are fine for the course forum.

Email to the instructor or TA will be answered if possible, typically within one business day—if you want short turnaround time, go to office hours. The best kinds of questions to ask via email are those that require short answers but are irrelevant to others in the class. Questions like “why doesn’t my program work?” and “please explain this concept to me” are too difficult to answer via email, and are best asked and answered in person at office hours.
Academic Honesty

This is a class on computer security, so ethics are of the utmost importance. You must follow these two simple commandments. If you are caught doing any of these things, there will be very serious consequences (see below).

1. Thou shalt not represent others’ work as your own.
2. Thou shalt not attempt to break into computer systems without prior written permission from the computer’s owner.

Unacceptable Behavior

This class is about computer security, and I encourage you to experiment with computing exploits—often, the best way to learn about something is by doing it. However, you must obtain WRITTEN PERMISSION before you experiment on any computer system that you do not personally own. THERE ARE NO EXCEPTIONS TO THIS RULE! If I find that you have disrupted someone else’s computer or network without their written permission, you will immediately fail the class and I will refer the case to campus authorities and/or the police. This may seem excessive, but written permission is the only thing that’ll hold up in court, and attempts to hack into others’ computing systems can easily end up there.

Plagiarism

Plagiarism in any form is completely unacceptable. Plagiarism is defined as “the unauthorized use or close imitation of the language and thoughts of another author and the representation of them as one’s own original work.” [dictionary.com] It’s not plagiarism (or academic dishonesty) if you acknowledge your sources, though if the assignment says to do something yourself, you won’t get credit for turning in someone else’s work even if you acknowledge it properly. The moral here: always acknowledge your sources!

Plagiarism will be assumed, until disproved, on work that is essentially the same as that of other students. This includes identically incorrect, off-the-wall, and highly unusual duplicate answers where the probability of a sheer coincidence is extremely unlikely. All parties to this unacceptable collaboration will receive the same (zero) score. In the case of programs, reordering routines, renaming files, and simply renaming variables does not make two programs different. Remember—a zero score on either exam or on the term project is grounds for failing the course. Those caught cheating will get a zero score on the assignment or exam and will be referred to their Provost. I reserve the right to take stronger action at my sole discretion, such as giving you an F in the class, should the situation warrant it.

You may discuss homework with your friends, but you are expected to abide by the Simpsons rule—the only thing you may bring to such a discussion is you, and no written notes may be taken away from the meeting. Your discussions must focus on concepts covered in class or assigned in the homework, but you may not discuss specific details from the homework. Looking at, modifying, or copying each other’s files or solutions is strictly forbidden. If you’re unsure of what is and is not allowed by this policy, please talk to me before doing something that might be considered cheating.

The Simpsons rule also states that, following any class-related discussion, you must take a break for at least half an hour (e.g., by watching The Simpsons or Mythbusters) before doing further class work. Reading something unrelated to CMPS 122 also qualifies. See me if you’d like suggestions for non-computer science reading material.