

# CS 444/544 Introduction to Cybersecurity, Spring 2011

**Instructor:** Jed Crandall, jedcrandall@gmail.com

*Never hesitate to email me directly about anything.*

**Office and office hours:** FEC 335, Tuesdays/Thursdays 10:00am to 11:00am, Wednesdays 2:00pm to 3:00pm.

**Prerequisites:** None formally, having taken several 300-level CS classes before this class is highly recommended. If you're uncomfortable with low-level systems programming or haven't learned about stuff like virtual paging or system calls then come talk to me early in the semester.

**TA:** You're all TAs! Just kidding, but the labs will be challenging, so you are encouraged to help each other out. Feel free to use the mailing list for asking questions and giving pointers.

**Mailing lists:** There are two mailing lists, one list that you are required to join that only I will post on, and I will only post important class announcements to that list. There is also a chat list, which is optional but highly encouraged, for students to share ideas and thoughts, things they see in the news, ask questions, get help on labs, etc. Discouraging other students from posting to this list will not be tolerated, if you feel someone is abusing the list let me know privately and I'll deal with it, or simply remove yourself from the mailing list.

**Course website:** <http://www.cs.unm.edu/~crandall/444544spring2011/>

I'll post lots of important stuff here, like the lab assignments, links to the mailing lists and Google calendar, grades, etc.

## **Required texts:**

1. *Computer Security: Art and Science* by Matt Bishop (the brown graduate version, don't buy the green version with a different title)
2. *Gray Hat Hacking, 2nd. Edition* by Shon Harris *et al.* The third edition is probably okay if you'd prefer the newer edition.

**Class meeting time and place:** Mondays 2:00pm to 5:00pm in ME 300. Attendance is required and is part of your grade. There will usually be a lecture in the first 30-50 minutes of the class, and the rest of the time will be lab. We'll usually take a 15-minute break sometime during the 3-hour period.

**Grading:** For letter grade purposes, below 60 is an F, 60 and up is a D, 65 and up is a C-, 70 and up is a C, 75 and up is a C+, 80 and up is a B-, 82 and up is a B, 85 and up is a B+, 87 and up is an A-, and 90 and up is an A. I only give A+'s in extreme circumstances.

Only two things factor into your final grade: attendance and labs. I'll just combine them as percentages, with your grade being 60% labs and 40% attendance, and then assign a letter grade as described above. There is no midterm or final, and reading assignments are not graded formally.

**Labs:** Each lab assignment will state how many points it's worth, typically 100. I anticipate about 7 or 8 lab assignments total this semester. I'll add up your total and divide by the total number of points possible, and that will be the lab part of your grade.

**Attendance:** Because of the lab-oriented nature of this class, we meet 14 times this semester. Thus it's very important to make use of this time and for you to show up. I'll take role each meeting. Each attendance day is worth five points, with deductions for the following kinds of things:

1. Being late (more points for being more late)
2. Leaving early
3. Coming back from 15-minute breaks late
4. Using any device (the lab computers, your laptop, your cell phone, etc.) for anything not related to what we're doing in the class, like checking your email or Facebook or whatever

I'll allow up to two excused absences per student, but you need to notify me well before the absence and get my permission to miss class. Emergencies can also be excused absences, at my discretion.

**UNM statement of compliance with ADA:** "Qualified students with disabilities needing appropriate academic adjustments should contact the professor as soon as possible to ensure your needs are met in a timely manner. Students must inform the professor of the disability early in the class so appropriate accommodations can be met. Handouts are available in alternative accessible formats upon request."

### **Cheating and collaboration:**

I'll try to clearly state on each lab what constitutes cheating and what kind of collaboration I expect for that lab. It will be different for each lab. If you have any questions, be sure to raise them. In general, I want you to help each other as much as possible but in this class if you find yourself repeating something rather than reporting it as a result of your own efforts then you're probably doing something wrong.

### **Group work:**

In general, I'll try to structure most of the labs so that it's difficult for group members to free-load. Sometimes I'll assign groups, sometimes you'll pick your group members, and sometimes you'll work in groups but turn in whatever deliverables individually. If you're having any problems with your group, like a particular member isn't doing what they're supposed to do or your group is not involving

you in discussions or meetings or not giving you anything to do, it's important to let me know as early as possible.

### **Lab policies:**

A separate document titled "Lab Policies" will be handed out after the ethics portion of the class is complete. You must read this document before signing the ethics form and getting an account in the lab environment or receiving any laptops or hard drives. That document should be considered an addendum to this syllabus.

### **Topics to be covered:**

Computer security and privacy is a very broad field that ties into nearly all areas of computer science, and is constantly changing, so we'll focus on what I see as the core ideas of security of privacy. After this course it's my hope that you'll be able to go to a security and privacy conference (such as Oakland, CCS, NDSS, or USENIX Security) and understand most of the papers there. We'll focus on the following:

- Ethics, legal issues, and human factors
- Security policies and mechanisms
- Security mechanism flaws and vulnerability classifications
- Secure design principles
- Abstractions of how information flows, both explicitly and implicitly
- Cryptography and trust relationships
- The theory of computer and network security and privacy
- Emerging research areas