

CS 444/544 Introduction to Cybersecurity, Spring 2013

Instructors: Tony Espinoza, amajest@cs.unm.edu
Jed Crandall, jedcrandall@gmail.com

Never hesitate to email either of us directly about anything.

Office and office hours: Jed FEC 335, Tuesday/Thursday 3:15-4:45
Tony FEC 337, Tuesday/Thursday 3:15-4:45

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 us early in the semester.

TA: TBD

Mailing lists: There are two mailing lists, one list that you are required to join that only Jed and I will post on, and we 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 us know privately and we'll deal with it, or simply remove yourself from the mailing list.

Course website: <http://www.cs.unm.edu/~amajest/444544spring2013>

Important stuff will be posted here, like the lab assignments, links to the mailing lists, 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. *Hacking The Art of Exploitation, 2nd. Edition* by Jon Erickson

Each student is responsible for obtaining a physical of each book.

Class meeting time and place: Tuesday, Thursday 2:00-3:15 CENT B146.

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. A+'s are only given in extreme circumstances.

Grades will be based on homeworks, labs, tests and attendance. The final and midterm are 10% each, attendance is 30%, homework 15% and labs 35%. All homework and lab assignments need to be submitted to cs444544spring@gmail.com not our personal email accounts.

Homeworks will be a mixture of reading assignments and coding assignments.

Labs: Each lab assignment will state how many points it's worth, typically 100. We anticipate about 2 or 3 lab assignments total this semester.

Attendance: There will be a sign in sheet each day and you have until 5 after to sign in before the sheet is put away and you are considered absent. Deductions to your attendance grade will also be made for:

1. Leaving early
2. 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

Two excused absences per student are allowed, but you need to notify one of us well before the absence and get my permission to miss class. Emergencies can also be excused absences, at Jed's 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:

We'll try to clearly state on each lab what constitutes cheating and what kind of collaboration is expected for that lab. It will be different for each lab. If you have any questions, be sure to raise them. In general, we 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, we'll try to structure most of the labs so that it's difficult for group members to free-load. Sometimes we'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 us know as early as possible.

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