CS 444/544 Introduction to Cybersecurity, Spring 2012

Instructors: Roya Ensafi (royaen@cs.unm.edu) and Jed Crandall (jedcrandall@gmail.com)

Never Hesitate to email us directly about anything. If you are emailing us about your group assignments, always cc the members of your group unless there's some reason for privacy.

Take responsibility for what you do. If you learn something in the class and misuse it, you are the one responsible for that act.

Prerequisites: Not formally.We strongly recommend that students to have taken CS 341 (computer organization and design) and CS 361 (data structures and algorithms), or have a basic understanding of things like system calls, assembly language, data structures such as graphs and trees, and computational complexity before taking 444/544. If you have doubts, contact the instructors.

Class meeting time and place: Mondays, Wednesday, and Fridays from 4:00pm to 5:00pm in Centennial Engineering Center room B146A. Attendance is required and is a part of your grade.

Office and office hours: FEC 343/335, Mondays, Wednesdays, and Fridays from 8:30am to 9:30am. If you need to meet us and can't make it to office hours, email us for an appointment.

TA: The TA is Mike Jacobi . He will attend class regularly. He will mostly help out with system administration-type duties and programming parts of labs, so won't be holding office hours.

Required texts: *Computer Security: Art and Science* by Matt Bishop (the brown graduate version, don't buy the green version with a different title), *Gray Hat Hacking: The Ethical Hacker's Handbook, 3rd Edition* by Shon Harris *et al.* We recommend buying hard-copies of the books, since we can't accommodate students who use PDFs of the book during open-book tests (unless there are special arrangements, *e.g.*, with the UNM testing center for that specific student).

Mailing lists/ Blog info: There will be two mailing lists, one required and one optional. See the course website for details. There is also a blog (http://cs444544.blogspot.com/) to share ideas and thoughts, things you see in the news and think it will be interesting to others. Discouraging other students from posting to mailing list and blog will not be tolerated, if you feel someone is abusing the list let us know privately and we'll deal with it.

Course website: http://www.cs.unm.edu/~royaen/444544spring2012
We will post lots of important stuff here, like lab assignments, links to the mailing lists, Google calendar, grades, *etc.*

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. We only give A+'s in extreme circumstances.

Four things factor into your final grade: labs, attendance, midterm exam, and final exam. We will combine them as percentages, with your grade being 60% labs, 20% attendance, 10% midterm, and 10% final. We reserve the right to curve the overall grades at the end of the semester, if we decide not to curve then they reflect the amount of effort students put into the class. *The difficulty of labs and exams will be different for 444 students compared to 544 students. 544 students will be expected to answer more open-ended exam questions and have more research novelty in their final project.*

Labs: Each lab assignment will state how many points it's worth, typically 100. There will be 4 main labs, that will help you learn main security topics in practice. We'll add up your total and divide by the total number of points possible, and that will be the lab part of your grade. Programming is encouraged, C, Perl, and Python are recommended. You may use other scripting languages(*e.g.*, Ruby), but keep in mind that we won't be able to help you as well in languages we don't know as we can in languages we do. Be sure to start early on the lab assignments and get the help you need to get them done.

Late assignments will be accepted only in special circumstances (medical, etc.).

Attendance: We will meet three times a week this semester. Your grade for attendance will be the fraction of regularly scheduled lecture periods for which you are present. There will be a "sign up" sheet until 5 minutes after class starts which you have to sign every session. We may mark you not present, without immediately notify you, for any of the following reasons:

- If you don't show up to that class
- If you are more than 5 minutes late (no sheet to sign)
- If you are 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, Facebook, *etc.*

Two "not present" days will be dropped at the end of semester. Things like medical emergencies, attending conferences, *etc.*, may be considered excused absences (*i.e.*, not count against your grade) if you notify us about them in a timely manner.

Midterm exam: The midterm will be on Monday, 12 March in the class at the regular time.

Final exam: The final will be on Monday, 7 May, from 5:30pm to 7:30pm.

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, personal statements: Most labs are done in a group. You and your group members are expected to do your own lab setups, collect your own data, and write your own lab writeups. Doing labs can be as hard as you want them to be, so if you think the lab is easy for you, we are sure you are not doing a good job in it. We don't care if you share source code or grab source code from any place you find. However, if you do so, you have to clearly delineate it and attribute it properly to its source. Repeating the work and materials of others as your own will not be tolerated in this class and will be considered cheating. Remember, everything you write in English language, and all ideas that you present as your own in the writeups needs to be original material by you. If you copy and paste any material (text, figures, *etc.*) from any source, you must explicitly reference to the source.

Each lab assignment will have specific instructions about what is acceptable in terms of cheating and collaboration. Be sure to read it, and if you don't understand it you are responsible to ask us. Excuses such as "I didn't know" is not acceptable.

Each test will state at the top what materials you're allowed to use (book, notes, *etc.*). Anything not specified as open is closed. In other words if the test instructions don't say "open-cheat-sheet", assume the test is closed-cheat-sheet.

All university policies regarding these matters will be strictly enforced. Typically we'll give the cheating party or parties a 0 on the assignment, but we may pursue further action in some cases pursuant to University policy.

In group-based labs, everyone needs to contribute. If some group members do all the work and others slack off, we consider that a fault of each and every member if the group individually. Doing all the work yourself in not an alternative to showing leadership. If you have any problem in this regard and need help, send us email as soon as possible. Every group member will attach a personal statement to the final submitted lab writeup stating their contributions. All members of the group must be “cc”ed when you submit the form to us. If another group member claims a contributions that they didn’t actually make, your two options are (1) ask them to change their personal statement, or (2) tell us about it privately, we know how to deal with it. Personal statements should answer the following questions:

1. What ideas did you contribute to the lab?
2. What tangible contributions did you make (source code, writing, implementation, experimental testing, etc.)? “Tangible” means that if we ask you to show that to us you can show it to us.
3. In what instances did you show leadership for group (motivating people to work, helping them learn something, organizing meetings, *etc.*)?

If your personal statement is misleading in any way, that can be considered cheating, so make sure your personal statement is clear and truthful. We reserve the right to call any student into our office and ask them questions about their personal statement and technical questions about the lab itself before giving a grade for the personal statement.

Our expectations of you as students:

- **Be studious:** come to class, come on time, stay on task, take time to make sure they understand things well, *etc.*
- **Take responsibility for your own learning**: if you find that coming to class is a waste of time, then you are not taking responsibility for your own learning. Do NOT expect us to spoon-feed you information that is already in a well-known book that you can read it by yourself. Our goal is to teach you how to learn things that nobody knows yet. A philosophical approach for you to take in this class is to “teach the teacher, surprise us.”
- **Do only excellent work:** anything worth doing is worth doing well. Think before you start your experiments, always know exactly why you do what you are doing. You’ll be better off giving us a 5-page report that is well-written, clearly stated, and compelling than 15 pages of nonsense. When you are writing your report, for each sentence ask yourself why you are writing that and how it can help us in understanding you. Keep it simple and make sure everything you do is excellent.
- **Show leadership and be a mentor:** don’t do only what we ask you to do, do more, learn more, and try to teach your group members more. If someone in your group is not as strong as you in some topics, help them learn and motivate them to get things done instead of doing it yourself.
- **RTFM:** read the manual. We don't mind at all when students ask us questions that they could get the answer to from the man pages, but it's a bad habit since a good gray hat hacker always checks the man pages first.

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 we see as the core ideas of security of privacy. After his course it's our hope that you'll be ready to work in this field and go to a security and privacy conference (such as Oakland, CCS, NDSS, or USENIX Security) and understand most of the papers there.

Topics that we will cover are (1) ethics, legal issues, and human factors, (2) security policies and mechanisms, (3) security mechanism flaws and vulnerability classifications, (4) secure design principles, (5) abstractions of how information flows, both explicitly and implicitly, (6) cryptography and trust relationships, (7) the theory of computer and network security and privacy, (8) emerging research areas.