CS 4235, Introduction to Information Security, Spring 2014
Syllabus

This course is a broad overview of computer security. Topics include security principles, cryptography, network security, secure coding, malware, operating system security, privacy, and security policy. Students taking this course should have a solid undergraduate background in computer theory, computer programming, computer networking, operating systems, and mathematical maturity.

Instructor

Joel Odom odom@gatech.edu
Office: 250 14th Street (GTRI Building), Office 321 (Moving to Tech Square Mid-Semester)
Office Hours: Tuesdays Immediately After Class in Clough Room 146 (Unless Otherwise Noted)
Teaching Assistant: Wei Meng wei@gatech.edu

Resources Used

The advertised textbook for this course is *Security in Computing* by Pfleeger & Pfleeger, however the majority of the material in this course will be drawn from different sources. Students are not required to purchase a copy of the advertised textbook. Lecture attendance is critical as most of the information that you will be responsible for will be presented in the lectures, not in the textbook.

Official announcements, homework postings, resource postings, and grade postings will be on T-Square. We will use Piazza for question and answer forums.

https://piazza.com/gatech/spring2014/cs4235/home

Students may e-mail the instructor directly with personal questions. Questions of a general nature should be posted on Piazza. I will generally check Piazza once or twice each weekday. Note that I'm not often online evenings or weekends, so please don't wait until the last minute to ask an important question, especially considering that posts made evenings or weekends will probably not be answered by me until I arrive in the office the next business day.

Readings, both required and supplemental will generally be available via T-Square. Some worthwhile books include:

Mark Stamp, *Information Security*, 2nd Ed
Ross Anderson, *Security Engineering*, 2nd Ed
Katz & Lindell, *Introduction to Modern Cryptography*

(Much of my lecture material will be drawn from the above books in addition to the Pfleeger book.)

Grading

This class will be graded on a points system. Points accumulate over the semester until you reach a final total at the end of the class. Final grades will be assigned based on the percentage of final (non-bonus) points available that you receive. You need 90% to receive an A. 80% for a B. 70% for a C. 60% for a D. Planned points will be given for:

20 Points Each for Five Homeworks (100 Points Total)
20 Points Each for Two Quizzes (40 Points Total)
40 Points for Panel Discussion Project
60 Points for One Cumulative Final Exam
20 Points for Attendance & Participation (Based on Instructor's Subjective Judgement)

If quiz or exam grades are lower than expected I will apply an appropriate correction to ensure that grades are fair for unexpectedly difficult tests. I will publish statistics to help students evaluate their relative performance. Bonus points may be awarded for going above-and-beyond the basic responsibilities of the class. For example, students who ask a question that the instructor cannot fully answer may be offered the opportunity to research the topic for bonus points. *Cheating will not be tolerated.*

Schedule (Subject to Change)

Week	Topic	Assignment
1	Introduction	Read Emerging Cyber Threats Report
2	Cryptography I	
3	Cryptography II	
4	Cryptography III	Homework One Due (Symmetric Cryptography)
5	Access Control	
6	Network Security Protocols	Homework Two Due (Asymmetric Cryptography)
7	General Network Security	Quiz One
8	Web Security	(Week of Drop Day)
9	Secure Coding, Malware	Homework Three Due (Network Security)
10	Secure Computer Systems	
11	Operating System Security	Homework Four Due (Metasploit & Secure Coding)
12	Technical Leftovers	Quiz Two
13	Privacy, Policy	Panel Discussion Report Due
14	Panel Discussions	Homework Five Due (Reverse Engineering)
15	Panel Discussions	