CSC650   SECURE NETWORKED SYSTEMS
SPRING 2016

Fully secure systems don't exist today and they won't exist in the future.
                                                                    ~Adi Shamir

Instructor:	Hao Yue
Class Time/Location:	Tuesday, 7:00PM-9:45PM, Thornton Hall 429
Office:	TH 930
Office Hours:	Wednesday 11:00AM-12:00PM and 5PM-6PM, or by appointment
Email:	haoyue@sfsu.edu
TA:	TBA
Pre-requisite:	Grades of C or better in CSC 415; a good working knowledge of the C/C++ programming language
Textbook:	Network Security: Private Communication in a Public World, 2nd Edition Charlie Kaufman, Radia Perlman and Mike Speciner

Course Description

Computer and network security is one of the most exciting and challenging areas in all of computer science, which has also become one of the most serious concerns amongst industry and government. This course introduces the fundamental concepts on computer security and standard security mechanisms and protocols. Topics covered in this course include Secret Key Cryptography, Public Key Cryptography, Authentication, Network Security, Intrusion Detection, DDoS, Web Security, DES, RSA, IPsec, SSL/TLS, and other emerging topics.

Learning Outcomes

At the end of this course, students will
- Have basic knowledge on cryptography and standard network security mechanisms
- Gain hands-on experience in implementing security mechanisms and building secure systems

Course Expectations

The students are expected to attend every class, actively and constructively participate in

class discussions, do the readings assigned for class, and complete all homework and project assignments on time.

Grading

The grading policy is as follows:

- 10% Attendance and Quizzes
- 15% Homework Assignments
- 20% Course Projects
- 25% Midterm Exam
- 30% Final Exam

At the end of the semester, each student will receive a final score out of 100, which will then be converted to a letter grade based on a class curve.

Assignments

There will be three homework assignments and two project assignments in this course. Each homework assignment counts for 5% of the final grade, and each project assignment counts for 10%. All assignments are due at the announced deadlines. Students are allowed to make late submission within 48 hours of an assignment deadline, for 75% of the credits. Submissions later than that will not be accepted, and it will result in a zero for that assignment.

Exams

The course will include one closed-book, closed-notes midterm and one take-home final exam. Students will be responsible for material covered both in the readings and in the lectures. Attendance is therefore recommended as not all class discussions will be covered in the text. If you are unable to attend the midterm, you MUST contact the instructor at least one week before the exam. If you have acceptable and documented excuses, you may be given a make-up exam. Any other exam absence will result in a zero for that grade.

Attendance and Quizzes

Attending classes regularly is required. There will be five roll-calls in this semester, and each of them counts for 1% of the final grade.

Quizzes will be assigned sporadically throughout the term and test comprehension of the previous class, which count for 5% of the final grade in total. Being late for or missing a quiz without an extremely sound reason will result in a zero for it.

Class participation will be a measure of contributing to the discourse through discussion and questions, both inside and outside of class. The goal is for thoughtful contributions that show engagement with the material. Students actively participating in class will receive up to 5 bonus points in the final grade.

Academic Integrity Policy
Cheating and plagiarism are serious violations of the academic code of conduct. Students who have been found to be cheating with be notified by the professor. Furthermore their act will be reported to the Office of Student Conduct (OSC). Please consult the departmental policy on plagiarism/cheating at http://cs.sfsu.edu/plagarism.html.

Students are not allowed to share their homework solutions or any work with other students, unless permission from the instructor is given. Submitting someone else's work as your own is considered cheating. Letting someone else submit your work as her/his own is also considered cheating, and will be treated equally.

If you wrote your code on your own, you must be able to explain its details. If you are unable to explain the details of code that you turned in, I consider this a strong indication that you did not write the code on your own; in that case, I have the option of giving you a zero on that assignment, and reporting the incident to the department chair.

Depending on the seriousness of the offense, students caught cheating could be assigned an "F" in the course, or be expelled from school.

Accommodations for Students with Disabilities
Students with disabilities who need accommodations for exams are encouraged to contact the instructor. The Disability Programs and Resource Center (DPRC) will facilitate the accommodation process for individuals with verified disabilities. If a student is a DPRC client, he/she must present an RAV (Reasonable Accommodation Verification) and an EAR (Exam Accommodation Request) to the instructor at the beginning of the semester. Students are responsible for submitting the completed EAR form to the DPRC. Any changes to the accommodation require prior approval by a DPRC specialist. Changes cannot be requested during an exam. The DPRC is located in the SSB-110 and can be reached by telephone (voice/TTY 415-338-2472) or by email (dprc@sfsu.edu).

Course Schedule

Date	Topic	Assignment	Reading
02/02/2016	Syllabus Introduction		Syllabus
02/09/2016	Intro to Cryptography Secret Key Cryptography	Homework 1	2.1, 2.3, 2.4 3.1-3.3
02/16/2016	Secret Key Cryptography Hash Function	Project 1	4.1-4.3 5.1-5.2
02/23/2016	Public Key Cryptography	Homework 1 Due	6.1-6.4
03/01/2016	Authentication	Project 1 Due Homework 2	9.1, 9.3-9.7
03/08/2016	Social Engineering Midterm Review	Homework 2 Due	
03/15/2016	Midterm (7:00-9:30PM)		
03/22/2016	No Class – Spring Recess		
03/29/2016	PKI	Homework 3	15.1-15.5
04/05/2016	Internet Security	Homework 3 Due	17.1, 17.3, 18.5, 18.6
04/12/2016	Intrusion Detection	Project 2	
04/19/2016	Web Security		25.1-25.6
04/26/2016	DDoS		
05/03/2016	Wireless Network Security	Project 2 Due	
05/10/2016	Review/Wrap up		
05/19/2016	Final Exam		

*Note that this is the preliminary schedule, which may be altered as the term progresses.