Course Syllabus

CS 558: Introduction to Network Security, Spring 2014
Computer Science, Boston University

January 15, 2014

1 Administrative

1.1 Official Description

Cryptographic tools: shared and public key cryptography, encryption, key exchange, and signature. Applying these tools in protocols and systems: confidentiality, authentication, data integrity (Kerberos; SSL/TLS, ISPEC; VPNs; certificates, PK). Firewalls, intrusions, viruses.

1.2 Actual Description

The official course description is out of date.

This course provides an introduction to the basic principles and techniques of building secure information systems. The focus of the course is network security, web security, and privacy, and will also cover basic cryptography. Broader social, legal and political aspects of security will also be touched upon, including issues relating to censorship, surveillance and information control.

This is meant to be a first course in information and network security. No background in networking or cryptography will be assumed. The only prerequisite is CS210 (or permission of the instructor). CS237 or equivalent course in basic probability is helpful but not required.

1.3 Course Staff.

CS558 Lectures:	Tuesday, Thursday 9:30-10:00 AM in CAS 116
CS558 Discussions:	Friday 9:00-10:00 AM in MCS B19 OR Friday 11:00-12:00AM in SCI 115
Prof. Goldberg's Office Hours:	Thursdays 3:30-4:00 and 5:00-7:15 PM in MCS 135C
Ethan's Office Hours:	Mondays 9:00-11:00 AM in MCS 135A
Assignments due:	11:59PM on Mondays, or as directed by the assignment.

1.4 Textbooks.

There is no course textbook. However, readings will be assigned, and sometimes handouts will be given out in class. The following textbooks are good references, but are not required.

- J. Katz and Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC Press. August 2007.

- Ross J. Anderson. Security Engineering. Wiley. 2008. Available FREE online at `http://www.cl.cam.ac.uk/~rja14/book.html`.

2 Course Timing and Communications.

CS558 Lectures:	Tuesday, Thursday 9:30-10:00 AM in CAS 116
CS558 Discussions:	Friday 9:00-10:00 AM in MCS B19 OR Friday 11:00-12:00AM in SCI 115
Prof. Goldberg's Office Hours:	Thursdays 3:30-4:00 and 5:00-7:15 PM in MCS 135C
Ethan's Office Hours:	Mondays 9:00-11:00 AM in MCS 135A
Assignments due:	11:59PM on Mondays, or as directed by the assignment.

Lecture attendance is required. Discussion attendance is highly recommended.

You are responsible for all material covered in lecture. Course topics, reference material, and scheduling (calendar) will either be discussed in class or posted on the course website. We will use piazza to communicate with you; please check piazza and the course website regularly. "I did not check piazza" will not be a valid excuse.

You are welcome to use Piazza to set up study groups, to post interesting security incidents you read about (please tag these as `interesting_incident_in_the_news`), or to discuss the course with other students. The piazza site is here:

`piazza.com/bu/spring2014/cs558`

If you have a question about the course you should:

1. Come to Prof. Goldberg (for questions about course material) or Ethan's office hours (for questions about assignments), OR
2. Post to Piazza.

Questions posted to Piazza will be answered by the course staff on Friday, Sunday, and Monday, and on a best-effort basis throughout the rest of the week.

You should only use email to communicate with the instructors as a last resort.

If you need to talk to the course staff in private, you can send us a private message on Piazza to let us know that you want to have a private conversation during office hours. You should not expect a response; instead assume we have read your message and you should then just show up at office hours. If you want to talk to one of us in person but absolutely can't make office hours, please send the relevant person an email with **at least three different options** for when you are available to meet.

3 Evaluation

The majority of your grade will be based on projects, assignments and presentations. There is one midterm covering the first 2/3 of the course and no exam. We reserve the right to deviate from the following grading formula.

Homeworks & Labs	40%
Security News Presentation	10%
Midterm	30%
Final Project	15%
Participation	5%

3.1 Lectures and Participation.

Participation will be based on attendance, asking good questions during security news presentations and lectures, answering questions on Piazza, during discussions, etc.

You are expected to be an active participant in class. **No messaging or surfing is allowed in class.** All electronic devices including phones, tablets and laptops must be silenced and put away unless being used for note taking, or as part of an in-class demo or assignment. If you are using them for any other purpose you will be asked to leave class. **If you are using them for note taking, then you will be required to private message (on Piazza) an electronic version of your notes to the professor at the end of the lecture.**

3.2 Homework, labs, presentations, and final project

Homework, labs, presentations, and final project will make up the bulk of the grading in this course. The final project and security news presentations are discussed in a separate handout.

Homeworks are generally pencil-and-paper exercises, while labs involve a significant problems-solving, programming, or data-analysis efforts. Please note that homeworks and labs will *not* be equally weighted, as some will be more substantial than others. The exact list and weighting of assignments is TBA.

Late assignment. You start the semester with a credit of 3 late days. For the purpose of counting late days, a "day" is 24 hours starting at 11:59PM on the assignment's due date. Partial days are rounded up to the next full day. You are free to divide your late days among the **homeworks and labs** any way you want: submit three assignments 1 day late, submit one assignment 3 days late, etc. After your 3 days are used up, no late submissions will be accepted and you will automatically receive 0 points for each late assignment. Late days are not available for the presentation or final project.

SUBMISSION POLICY. Homeworks and Labs must submitted as a **PDF** electronically through web-submit by 11:59PM on the day they are due. You may choose to hand-write your assignment and then scan it in before submitting, or you may choose to type up the assignment and then convert it to a PDF. You are encourage to use LaTex – please email us if you would like a Latex template to use. **No format other than PDF will be accepted.** Please make sure the electronic version of your assignment is legible; illegible assignments will not be graded kindly.

Every submitted homework and lab MUST include the following information:

1. List of collaborators
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)

3. Number of late days used on this assignment

4. Total number of late days used thus far in the entire semester

If any of this information is missing, at least 20% of the points for the assignment will automatically be deducted from your assignment. See also discussion on plagiarism below.

Regrading. If you would like to request a re-grade of an exam question or an assignment, be aware that question or assignment will be completely re-graded (and potentially result in a lower grade). Regrading will be handled by the Teaching Fellow.

4 Important Dates

Please take note of the following dates and plan your travel accordingly.

Tuesday March 25, 9:30-11:00AM Midterm. The midterm will cover material from the first two-thirds of the course.

Friday March 28 Last day to drop course with a W. Midterm will be graded and returned by Wednesday March 26; if you are considering dropping the course, please make sure to see Prof. Goldberg during her special office hours on Wednesday March 26 or Thursday March 27.

Friday May 2, 9:00-1:00 PM CS558 open poster session; the CS department will be invited, and you are welcome to invite colleagues and friends.

5 Ethics

To defend a system you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy is that you must respect the privacy and property rights of others at all times, or else **you will fail the course**.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." Understand what this law prohibits.

Read BU's Conditions of Use and Policy on Computing Ethics (`http://www.bu.edu/tech/about/policies/computing-ethics/`) and the BU's Academic Conduct Code (`http://www.bu.edu/academics/policies/academic-conduct-code/`). As members of the university, you are required to abide by these policies.

6 Collaboration Policy

You are strongly encouraged to collaborate with one another in studying the course material. As long as it satisfies the following conditions, collaboration on the homework assignments is encouraged and will not reduce your grade:

- You may discuss ideas and approaches with other students in the class, but:

  - You may not share actual code. In other words, the code you write must be entirely your own, which you must write and debug without looking at other people's code. Don't permit others to copy your code.
  - You must write up your solutions completely on your own, without looking at other people's write-ups.

  You must also acknowledge clearly in your solutions people with whom you discussed ideas, either for your written solutions or for your code.

- You may not work with people outside this class (but come and talk to us if you have a tutor), get someone else to do it for you, etc.
- You are welcome to use any textbooks, online sources, blogs, research papers, Wikipedia, etc in your assignment, **as long as these are properly cited in any submitted work**. Failure to do this is plagiarism and is serious violation of the CAS Academic Conduct Code and basic scientific ethics, and will not be tolerated.
- You are not permitted to collaborate on exams.

It is your responsibility to know and understand the provisions of the CAS Academic Conduct Code.