CS558 Network Security.
Course Syllabus, Spring 2012

January 18, 2012

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 Prerequisites.

CS455 or permission of the instructor. CS237 or equivalent is strongly recommended.

1.3 Elaboration.

The official course description is a little out-of-date; not all topics listed above will be covered, while some new topics will be introduced. This course will require both mathematical maturity (especially with probability, so CS237 is strongly recommended), programming maturity, and basic understanding of networking (so CS455 or permission of the instructor is required).

The course will be divided into three basic "units". The following is a tentative list of topics for each unit, subject to change. Relevant references will be given at the beginning of each lecture and on the website.

1. **Data privacy.** An understanding of data privacy, as well as mathematical definitions of privacy. Topics include: Attacks on privacy and anonymity. K-anonymity. Differential privacy. (1 month)

2. **Basic crypto.** Basic crypto and techniques for rigorously arguing about the security of protocols. Topics include: block ciphers, message authentication, symmetric-key encryption, hash functions, public-key encryption, digital signatures. (2-3 weeks)

3. **Security in networks.** The security issues at various network layers of the Internet, and the protocols proposed and deployed to deal with these security issues. For example: Public key infrastructures and why they are difficult to deploy in practice. DNS security. BGP security. Login security. IP and TCP security. etc. (Rest of the course.)

1.4 Course Staff.

Instructor: Professor Sharon Goldberg, `goldbe@cs.bu.edu`, MCS135 (111 Cummington St.)
Please make sure that all course-related email has "CS558" in the subject line.

Basic crypto lectures will be given by Dr. Adam O'Neill, `amoneill@gmail.com`, MCS 135 (111 Cummington St.)

1.5 Textbooks.

There is no course textbook. However, readings will be assigned.

1.6 Course Timing and Communications.

Lecture:	Monday, Wednesday 1:00-2:30 PM in CAS 221
Instructor's Office Hours:	Monday 3:00-6:00 PM in MCS 135

Lecture attendance is required. You are responsible for all material covered in lecture. Course topics and reference material will either be handed out in class or posted on the course website. We will use email to communicate with you. Please check your BU email regularly. "I did not check my email" will not be a valid excuse.

We encourage you to come to office hours. If you need to talk to one of us in person but absolutely can't make the office hours, please send us an email with at least three options for when you are available (for Professor Goldberg, please check her calendar at

`http://www.google.com/calendar/embed?src=sharon.goldbe@gmail.com`

before proposing a time).

2 Grading

The majority of the grading in this course will be based on projects, assignments and presentations. There is one midterm covering the first 2/3 of the course and no exam.

Assignments	45%
Midterm	20%
Poster	20%
Security News Presentation	10%
Participation	5%

We reserve the right to deviate from this formula.

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).

2.1 Security News Presentation

Each student will be required to give a 7 minute presentation on a topic related to security and privacy that has recently appeared in the popular news, the technical press, blogs, or advocacy websites (e.g., the EFF), with one student presenting every class. Presentations should be accompanied by a slide presentation. Unless you have an extraordinary presentation style (see, e.g., Ed Felten), no more than 5 slides should be used.

Presentations should cover both the "superficial" issues presented in the press, and also explain the underlying technical issues. For instance, a story about a hacker issuing fake SSL certificates should also include an explanation of what an SSL certificate is, why hacking it matters, and details about how the attack was carried out. Notice that obtaining all this information will require you to dig deeper than just what was presented in the popular press. Condensing this information down to 7 minutes will require some effort, so please plan accordingly.

Dates and adminstration. Presenters must email Prof. Goldberg with the topic of their presentation at least 1 week before their presentation dates. Presenters should arrive early on the day of their presentation to test the projector in the class room, and be ready to begin their presentation at exactly 1:30PM.

2.2 Assignments

Assignments will make up the bulk of the grading in this course. Please note that assignments will *not* be equally weighted, as some will be more substantial than others. While the exact list of assignments is TBA, some assignments will mostly involve programming, others will be written and involve mostly math and problem solving, others will involve writing summaries to assignment readings, and some may involve all three.

Submitting assignments. Assignments must submitted as a **PDF** electronically through websubmit. 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. 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.

Please make sure to reference your sources and your collaborators in every assignment! Assignments with no list of sources or collaborators will automatically be given a grade of 0.

Late assignments. 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 take-home assignments 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. **When submitting a late assignment, please indicate how many late days you are using.**

2.3 Poster

Students must work in *pairs* to prepare a poster on a topic in *network security*. Students must choose a topic in networking (examples from past years include Voice over IP, Vehicular Networks, text messaging, etc.), clearly state a security property that is important to that application, and either (a) present a protocol that guarantees that security property, or (b) present an attack on the application that breaks the security property.

Protocols and attacks need not be original; students are welcome to present attacks or protocols that were published at technical conferences or that appear in Internet Standards.

Original work. Extra credit will be given for original work. If you plan to do original work, please email Prof. Goldberg with the description of what you plan to do by March 19, 2012 at 9AM.

Poster check-in. Each pair must email Professor Goldberg by April 9, 2012 at 9AM with (a) the names of the people working on the poster (b) the topic of the poster, (c) the security property that you plan to study, and (d) a link to the source describing the protocol or attack you plan to present.

Poster session. The course will culminate in a poster session that will be open to the entire department on May 4 2012, from 1:00-4:00 PM. You are welcome to invite colleagues and friends.

2.4 Important Dates

Monday March 19, 9AM If you plan to submit original work as your poster, please email Prof. Goldberg with a description of your topic and research plan by this day.

Wednesday March 28, 1:00-2:30PM Midterm. The midterm will cover material from the first two-thirds of the course.

Friday March 30 Last day to drop course with a W. Midterm will be graded and returned by Thursday March 29; if you are considering dropping the course, please make sure to see Prof. Goldberg during her (extra) office hours on Thursday March 29.

Monday April 9, 9AM Poster check in. Please email Prof. Goldberg with your poster topic by this day.

Friday May 4, 1:00-4:00 PM CS558 open poster session; the CS department will be invited, and you are welcome to invite colleagues and friends.

2.5 Collaboration Policy

You are strongly encouraged to collaborate with one another in studying the textbook and lecture 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), **seek on-line solutions**, get someone else to do it for you, etc.

- You must clearly acknowledge any textbooks, online sources, blogs, research papers, Wikipedia, etc., that you used in in your assignment. Failure to do this is plagiarism and is serious violation of the CAS Academic Conduct Code and basic scientific ethics.
- You are not permitted to collaborate on exams.

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