CS558 Network Security.
Course Syllabus, Spring 2013

January 15, 2013

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The official course description is a little out-of-date; not all topics listed above will be covered, while some new topics will be introduced.

More and more of our data is being collected by both governments and private companies. There is increasing evidence of regimes using networking technologies to censor information. New policy and legal frameworks being developed to establish or curb online freedom. In light of these trends, understanding the technical aspects of privacy, anonymity, and online censorship becomes increasingly important for computer scientists.

This course will focus on these issues. We'll discuss attacks on privacy and cover notions of privacy, including differential privacy, k-anonymity, and others. We'll talk about tools for online anonymity, including Tor and others, as well as the technical means used for online censorship, including firewalls, deep-packet inspection, DNS poisoning, and BGP attacks. Basic notions from cryptography (encryption, authentication, etc.) will be introduced along the way.

Note that the focus of this course has changed slightly relative to previous years, but as before, a portion of the course will be taught in a seminar style, with course projects and student presentations.

1.4 Topics

The course will be divided into four 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. **Systems security.** Exploiting bugs in programs. Buffer overflows, return oriented programming, fuzzing. This portion of the course will follow David Seidman's lesson plan. (Month of January).

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. **Data privacy.** How privacy is changing online, and mathematical definitions of privacy. Topics include: Attacks on privacy and anonymity. K-anonymity. Differential privacy. Private information retrieval. Basics of multiparty computation and relationship to privacy.

4. **Security and censorship in networks.** The security issues at various network layers of the Internet, and the protocols proposed and deployed to deal with these security issues. This semester will have a particular focus on how security protocols make online censorship easier or more difficult for countries to achieve. Some topics include: DNS security, censorship and takedowns. ToR and network-layer anonymity. SSL and how it affects censorship and filtering. Public key infrastructures like the RPKI and how they consolidate control on the internet. Routing security and routing-based censorship. Etc.

1.5 Course Staff.

Instructor:	Professor Sharon Goldberg, `goldbe@cs.bu.edu`, MCS135C (111 Cummington St.) Please make sure that all course-related email has "CS558" in the subject line.
co-Instructor:	Professor Ran Canetti, `canetti@cs.bu.edu`, MCS135D (111 Cummington St.) Some lectures will be co-taught.
Systems security lectures:	David Seidman, `David.Seidman@microsoft.com`

1.6 Textbooks.

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

1.7 Course Timing and Communications.

CS558 Lectures:	Tuesday, Thursday 3:30-5:00 PM in CAS 237
Lectures joint with CS591:	Wednesday 1:00-2:30 PM in MCS B19
Instructor's Office Hours:	Tuesday 1:30-2:30 PM and Tuesday 5:15-7:15 PM in MCS 135

Lecture attendance is required. Some CS558 Thursday lectures will be replaced with joint lectures with CS591 on Wednesday, and may be taught by either Ran Canetti, or Sharon Goldberg.

You are responsible for all material covered in lecture. Course topics, reference material, and scheduling (calendar) 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 and the course website regularly. "I did not check my email" will not be a valid excuse.

I encourage you to come to office hours. If you need to talk in person but absolutely can't make the office hours, please send an email with at least three options for when you are available (for Sharon 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 7 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 1.5 weeks before their presentation dates, and attend office hours to discuss the topic of their presentation *at least* one week before the presentation is scheduled to take place. 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 on time.

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.

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.

SUBMISSION POLICY. Assignments must submitted as a **PDF** electronically through websubmit 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 assignment 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.

2.3 Poster

Students must 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. Students may work alone or in pairs.

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, 2013 at 9AM.

Poster check-in. Each pair must email Professor Goldberg by April 2, 2013 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 3 2012, from 1:00-4:00 PM. You are welcome to invite colleagues and friends.

2.4 Important Dates

Tuesday 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.

Thursday March 21, 3:30-5:00PM Midterm. The midterm will cover material from the first two-thirds of the course.

Friday March 29 Last day to drop course with a W. Midterm will be graded and returned by Monday March 25; if you are considering dropping the course, please make sure to see Prof. Goldberg during her office hours on Tuesday March 26.

Tuesday April 2, 9AM Poster check in. Please email Prof. Goldberg with your poster topic by this day.

Friday May 3, 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), 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.