CSc 59867 Capstone II: Applied Cryptography and Information Security
Spring Semester 2010
Professor Fazio

Course Description. In this two-semester course, students are grouped into teams to work on projects of practical importance in applied cryptography and information security. The first semester starts by covering the basic principles and practices of information security. Teams will pick a topic for their project, based on their interests and on discussions with the instructor. After reading a selection of papers on the chosen topic, each group will narrow down their focus and outline a working plan for the design, development, testing, evaluation, and deployment of their project. Teams will demonstrate their understanding of the principles and algorithms of their chosen area in a class presentation, and will prepare a project proposal with specific deliverables and milestones for the completion of their software project. The second semester will focus on the implementation of the proposed projects.

Course Objectives. Successful completion of this course trains students in the following directions: (1) how to approach moderately large software projects and work effectively in teams; (2) analyze, understand, and evaluate the security of computer systems; (3) gain insights on the use of cryptography to build security and privacy properties into real-world applications; (4) gain expository and presentational skills to prepare and deliver technical reports.

Required Text. No required textbook. Lecture notes and relevant papers will be posted on the course webpage (http://www-cs.ccny.cuny.edu/~fazio/capstone0910/ay0910-csc59866.html).

Recommended Texts.

- Handbook of Applied Cryptography, by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Available online: http://www.cacr.math.uwaterloo.ca/hac/
- Security Engineering, by Ross Anderson. Available on-line: http://www.cl.cam.ac.uk/~rja14/book.html

Required Software. (1) NetBeans 6.5 (http://www.netbeans.org/downloads/6.5.1/index.html); (2) SunSPOT Manager (https://www.sunspotworld.com/SPOTManager/index.html).

Prerequisites. Senior-year students only, or permission by the department. Working knowledge of Java programming.

Major Topics Covered in the Course. Cryptography: Information security goals (data secrecy, data integrity, data origin); Basic primitives (one-way functions, cryptographic hash functions, block ciphers); Symmetric primitives (encryption, message authentication codes); Public-key primitives (asymmetric encryption, digital signatures); Cryptographic protocols (key exchange, key distribution, authentication); Advanced topics (identification schemes, commitment schemes, secret sharing schemes, threshold encryption/signature schemes. Sun Small Programmable Object Technology (Sun SPOT).

Team Projects. Projects will be written in Java, based on the SunSPOT technology.

Grading. Project implementation (40%), Project report (40%), Project Presentation (20%).

Office Hours. Mondays 2:00-3:00pm. Shepard Hall 279.