CS 2950-v: Topics in Applied Cryptography (Fall 2017)

Meeting Time: TTh 10:30-11:50

Location: CIT 506

Instructor: Seny Kamara (seny@brown.edu)

Office hours: Th 3:30-5

Course Home Page: http://cs.brown.edu/~seny/2950-v/

Prerequisites: CSCI 1660 required; CSCI 1510 strongly recommended.

Overview

This course surveys recent developments in applied cryptography. It is structured as a seminar where students present research papers to their peers and work on a semester-long research project. We will focus on research motivated by privacy and security issues that arise in practice from areas like cloud computing, databases, surveillance and finance. Topics will vary each year.

Though the course is motivated by practical/applied problems, some of the papers we will study are theoretical in nature. While previous exposure to the foundations of cryptography (including, e.g., provable security, the simulation paradigm, reductions) will be helpful, we will cover the necessary theory in class.

Topics (tentative)

This semester we will cover the following topics:

1. Encrypted systems: encrypted structures, encrypted algorithms, encrypted systems
2. Blockchains: crypto-currencies, practical consensus
3. Surveillance: exceptional access, lawful surveillance, subversion-resistance

Objectives

The goals of this course are for students to:

- understand how state-of-the-art cryptographic protocols work
- understand the tradeoffs achieved by various designs
- develop the ability to design cryptographic protocols
- develop the ability to analyze the security of cryptographic protocols

More general goals include:

- learn how to analyze the security of large cryptographic systems
- learn how to design practical cryptographic protocols
- learn how to effectively combine techniques and ideas from different areas of computer science
- learn how to read cryptography research papers
- learn how to pose research questions and formulate research problems

Course Materials

There is no textbook required for this course but students may find *Introduction to Modern Cryptography* by Katz and Lindell helpful to gain familiarity with cryptography. Other recommended (free) resources include

Introduction to Modern Cryptography by Bellare and Rogaway and *A Course in Cryptography* by Pass and Shelat.

Assessment

Grading will be based on weekly reading assignments, a paper presentation, a project and a project presentation.

Weekly reading (15%): Paper(s) to read will be assigned weekly and for every paper, students will be required to hand in a review consisting of the following:

- a summary of the paper
- a discussion of the paper's strengths
- a discussion of the paper's limitations
- two new research questions related to the paper

Reviews will be graded pass/not pass (late reviews will be counted as not pass).

Paper presentation (20%): Each student will present a (set of) research paper(s) to the class and will be evaluated on the following:

- Understanding: does the presenter understand the material?
- Related work: does the presenter know the related work?
- Insight and opinions: does the presenter have their own insight and opinions about the paper beyond what is in the paper?
- Clarity: is the presentation clear to the audience?
- Materials: are the slides or use of the whiteboard effective in supporting the presentation?
- Questions: can the presenter answer questions from the audience?

Project (40%): Projects can be either systems projects, theoretical projects or mixed projects. *Systems projects* will consist of an implementation of solution together with a thorough experimental evaluation. *Theoretical projects* will consist of designing a new protocol, together with a proof of security. Projects can be done collaboratively in groups of up to 3. *Mixed projects* will consist of designing a new protocol, a proof of security and an implementation. Larger teams will be expected to produce more substantial projects. Mixed projects should only be attempted in groups. We will provide a list of possible project ideas but you are also free to propose your own.

Feedback on projects will be provided throughout the semester. Teams will meet regularly with the instructor to get feedback on their progress. This includes a meeting at the start of the project to get approval on the project idea, meetings during the design and/or implementation stages and a practice talk with the instructor before the final presentation.

Teams will required to hand in a final project report that describes in detail the work they did. For theoretical projects this will include the design of the protocol and its proof of security. For systems projects, this will include design and architecture of the system and the experimental evaluation. For mixed projects it will include all the above.

Project presentations (10%): Projects will be presented to the class at the end of the semester.

Participation (15%): including attendance, in-class participation, peer project reviews and feedback.

Collaboration Policy

You are allowed and encouraged to discuss technical material with each other. You are also allowed to consult external sources including books, online material and other research papers for reviews, paper presentations and projects but all sources must be properly cited. All written/presentation work (i.e., paper reviews, slides, projects reports and project slides) must be entirely your work.

Credit Hours

Over 14 weeks, students will spend 3 hours per week in class (42 hours total). Required reading and weekly research questions is expected to take up approximately 7 hours per week (140 hours). In addition, researching and working on the final project is estimated at a total of approximately 40 hours over the course of the term.

Diversity & Inclusion

Our intent is that this course provide a welcoming environment for all students who satisfy the prerequisites. All members of the CS community are expected to treat one another in a professional manner. If you feel you have not been treated in a professional manner please contact either the instructor, Ugur Cetintemel (Dept. Chair), Tom Doeppner (Vice Chair) or Laura Dobler (diversity & inclusion staff member). We will take all complaints about unprofessional behavior seriously.

To access student support services and resources, and to learn more about diversity and inclusion in CS, please visit http://cs.brown.edu/about/diversity/resources/

Accommodations

Brown University is committed to full inclusion of all students. Please inform me early in the term if you have a disability or other conditions that might require accommodations or modification of any of these course procedures. You may speak with me after class or during office hours. For more information, please contact Student and Employee Accessibility Services at 401-863-9588 or SEAS@brown.edu.

Undergraduate students in need of short-term academic advice or support can contact one of the deans in the Dean of the College office. Graduate students can contact one of the deans in the Dean of the Graduate School office.