CS 2950-v: Topics in Applied Cryptography (Fall 2016)

Meeting Time: TTh 10:30-11:50

Location: CIT 316

Instructor: Seny Kamara (seny@brown.edu)

Office hours: Thursdays 1-3PM, CIT 507

Grad TA: Evgenios Kornaropoulos (evgenios_kornaropoulos@brown.edu). Office Hours: Wednesday 2-4, CIT 361

Undergrad TA: William Barclay (william_barclay@brown.edu)

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

Description: This course surveys recent developments in applied cryptography. Research in this field is motivated by privacy and security issues that arise in practice from areas like cloud computing, databases, surveillance and finance. Topics will vary each year.

Prerequisites: CSCI 1660 required; CSCI 1510 strongly recommended.

Overview

This fall, we will study the problem of *encrypted search*; that is, *how can we search on encrypted data?* In particular, we will be interested in how encrypted search techniques can be used to design *encrypted databases*.

As the technologies we deploy produce and consume an increasing amount of data, we are witnessing several conflicting trends. On one hand, these massive datasets are becoming more intrusive and privacy-sensitive and on the other they are becoming harder to secure. The latter is well-illustrated by the prevalence of data breaches and by the recent Snowden disclosures. Unfortunately, the standard tools at our disposal for enforcing data privacy and security, like encryption, eliminate the utility of many critical technologies such as databases, cloud computing, cloud storage, machine learning and data analytics. The area of encrypted search aims to solve this dilemma and reconcile these trends by producing a new generation of cryptographic primitives and systems that can secure data without eliminating its utility.

Though the course is motivated by practical/applied problems, some of the works 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)

1. Encrypted search engines and encrypted databases (EDB)
2. Solutions based on fully-homomorphic encryption (FHE)
3. Solutions based on oblivious RAMs (ORAM)
4. Solutions based on property-preserving encryption (PPE)
5. Solutions based on structured encryption (STE) and searchable symmetric encryption (SSE)
6. NoSQL EDBs
7. Relational/SQL EDBs
8. Inference attacks
9. Injection attacks
10. Locality and allocators
11. Academic systems
12. Industry systems

Objectives

The goals of this course are for students to:

- understand how state-of-the-art EDBs work
- understand the tradeoffs achieved by various EDBs
- understand the encrypted search techniques used to design EDBs and their limitations
- develop the ability to design EDBs
- develop the ability to analyze the security of EDBs

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 project and a project presentation.

Weekly reading (25%): paper(s) to read will be assigned weekly and for every paper, students will be required to hand in a brief summary and two new research questions related to the work. Summaries and questions will be graded pass/not pass.

Project (40%): projects can be either systems projects, theoretical projects or composite projects. *Systems projects* will consist of an implementation of an encrypted search solution together with a thorough experimental evaluation. *Theoretical projects* will consist of designing a new encrypted search solution, together with a proof of security. Projects can be done collaboratively in groups of up to 3. *Composite projects* will consist of designing a new encrypted search solution, a proof of security and an implementation. Larger teams will be expected to produce more substantial projects. In particular, composite 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.

Project presentations (20%): projects will be presented to the class at the end of the semester.

Participation (15%): e.g., scribing lecture notes, in-class participation, feedback on instructor notes, peer project reviews and feedback.

Note: For undergraduate students, grading will be done in collaboration with our UTA but final grades are always assigned by the instructor who will review the work himself. The instructor has the ultimate responsibility for final grades and to conduct any appeals processes.

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.

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.