CS 588: Security and Privacy in Networked and Distributed Systems

Course Description

This course will cover foundational concepts and advanced topics in privacy-enhancing technologies for connected and distributed systems. The content will focus on techniques for confidential communication, integrity, anonymity and reliability in networked systems. Additionally, the course will discuss challenges that arise in distributed setups with adversarial parties. Along the way, the material will introduce the necessary background in cryptography and show how cryptographic tools are used in real systems to provide the aforementioned guarantees.

The class is intended for graduate students who are interested in learning about the security and privacy challenges of modern (large-scale) systems. Class meetings will typically include regular instructions and discussions of offline reading resources. The content will cover material from textbooks and academic papers. Students are expected to complete a semester-long project, and present their work in class. Prior experience in security or privacy is not required but will be beneficial in better understanding the material

General Information

- **Instructor:** Anrin Chakraborti
- **Time:** Tue, Thu 5 PM - 6:15 PM
- **Location:** Burnham 308
- **Office Hours:** TUE 1:30 - 2:30 pm (otherwise by appointment/email)
- **Office hour Location:** SEO 1326
- **Email:** anrin@uic.edu (Piazza preferred)

Required Reading

There is no required textbook for the course. However, the material covered will be from the following sources

- A Graduate Course in Applied Cryptography by Boneh & Shoup

- Cryptography Engineering: Design Principles and Practical Applications by Ferguson, Schneier, Kohno (1^{st} edition)
- Research papers from recent security and cryptography conferences

Resources

We will primarily use blackboard for sharing course lectures and announcements. You may also refer to the course webpage which will have all the important dates. We will use Piazza for discussions. While all students are encouraged to attend office hours and ask questions, Piazza when used effectively can solve a lot of these problems with low overhead. Students will also be expected to participate actively in Piazza discussions.

Topics Covered (Tentative)

- Cryptography basics
- Distributed cryptography
- Authentication, PKI
- Passwords
- Encrypted messaging
- Anonymous communication
- Anonymous credentials
- Private storage
- Byzantine fault tolerance
- Distributed authentication
- Byzantine consensus
- Blockchains

Grading Criteria (subject to change)

- Warm-up assignment: 5
- Semester project: 70
- In-class quizzes: 20
- Class participation: 5

Course Policies

There are no allowed late days for submissions. If you are not able to make a deadline, please inform the instructor as soon as possible.

Attendance

Attending the lectures is highly recommended. If you miss a few lectures, don't expect to catch up easily with your peers. Please email me if you face an unexpected situation that may impede your attendance, participation in required class and exam sessions, or timely completion of assignments.

Honor code

As a student and member of the UIC community, you are expected to adhere to Community Standards (`https://dos.uic.edu/community-standards/`) of academic integrity (`https://dos.uic.edu/community-standards/academic-integrity/`), accountability, and respect. Please review the UIC Student Disciplinary Policy(`https://dos.uic.edu/wp-content/uploads/sites/262/2021/09/Student-Disciplinary-Policy-202` `pdf`) for additional information. We abide by these standards in this course. All the work you submit must be your own; you should not use paraphrasing software like (QuillBot), or AI software for writing (like ChatGPT), or any AI tool for content generation (spell-checkers are allowed) – unless explicitly allowed to do so. All cases of plagiarism will be referred to the Dean of Students office, and depending on the severity of the offense, you risk being dismissed altogether from the course. The Dean's office may further impose penalties including suspension and expulsion. If you have any question about whether some activity would constitute cheating, please feel free to ask.

Acknowledgements

This course has components that are inspired (directly or indirectly) by courses on cryptography by Prof. Michael Reiter, Prof. Jonathan Katz, and Prof. Dov Gordon at Duke University, University of Maryland, and George Mason University respectively.