EE599: Foundations of Secure and Private Computing: from Machine Learning to Blockchains

Units: 3
Spring 2020
Lecture: Tue. Thu., 2:00-3:20 PM,

Instructor: Salman Avestimehr
Office: EEB 504B
Office Hours: Tuesdays, 12:00-2:00
Contact Info: 213-740-7326. avestime@usc.edu.

Teaching Assistant:
Office: TBD
Office Hours: TBD
Contact Info: TBD

Course Description

This course provides a foundational view of the principles and algorithms for enabling secure and private computing, in particular for applications in machine learning and blockchains. The course consists of five main parts: (1) Information theoretic measures of security and privacy and basic cyphers for secure communication; (2) basic key exchange and public-key encryption; (3) secure and private multi-party computing; (4) secure and privacy-preserving machine learning; and (5) bitcoin and cryptocurrencies.

Learning Objectives and Outcomes

At the end of this course the students obtain a foudational understanding of key principles and algorithms for secure and private computing and communication. In particular, they learn the following topics: information measures for security and privacy; one-time pad and information-theoretically secure communication; stream cyphers; block cyphers; basic key exchange and public-key encryption; modular arithmetic and computationally hard problems; Diffie-Hellman public key encryption; secure multi-party computing; Yao's garbled circuit; oblivious transfer; BGW protocol; zero knowledge proofs; secure and private machine learning; federated learning and differential privacy; introduction to cryptocurrencies; nuts and bolts of bitcoin; overview of secure consensus protocols; proof of work and minining strategies; proof of stake.

Prerequisite(s): EE503 (or equivalent)
Co-Requisite(s): none
Concurrent Enrollment: none
Recommended Preparation: none

Required Readings and Supplementary Materials

- D. Boneh and V. Shoup, "A Graduate Course in Applied Cryptography", available online at https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_4.pdf.
- Papers and handouts that will be provided throughout the semester.

Description and Assessment of Assignments

Homework Policy

- There will be ~5 Homework assignments throught the course.
- Late HW will not be accepted. A late assignment results in a zero grade. Please have your homework turned in by the beginning of lecture on the date that it is due.
- Homeworks will be assigned on Thursdays and collected the following week in class (on Thursdays at the beginning of the lecture)
- Show your work in your homework solution; the correct answer alone is worth only partial credit.
- Homework collaboration is encouraged. This is discussing problems and solution strategies with your classmates, the TA, and/or the instructor and is to be distinguished from copying solutions of others which is prohibited.
- For computer-based assignments no code can be shared or copied from the internet. The only exception is code provided to the entire class by the instructor or TA.

Exam Policy

- The course will have 1 midterm exam on week 7. The exact date TBD.

Final Project Policy

- Proposals will be due two weeks after the midterm.

- Topics can be suggested by the students or taken from a list of suggested topics to be provided.
- The deliverables are:
    - A final report of approximately 5 pages.
    - A 20 min presentation to be made on a projects-day event at the end of the semester.

Grading Breakdown

- 10% participation
- 20% Homework
- 30% Midterm Exam
- 40% Final Project (including proposal, presentation, report)

Grading Scale

Final grades will be assigned by a combination of student score distribution (curve) and the discretion of the instructor. Final grades are nonnegotiable.

Grading Timeline

Homeworks and exams will be graded within two weeks of collection.

Course Schedule: A Weekly Breakdown

	Topics/Daily Activities	Readings and Homework	Deliverable/ Due Dates
Week 1	Course introduction; Introduction to cyphers; Information measures: entropy and mutual information.	Handouts will be provided.	
Week 2	One-time pad; information-theoretic secure communication; stream cyphers	Handouts will be provided. Hw 1 will be assigned.	
Week 3	Block cyphers	Handouts will be provided. Hw 2 will be assigned.	Hw 1 is due.
Week 4	Basic key exchange and public-key encruption	Handouts will be provided. Hw 3 will be assigned.	Hw 2 is due.
Week 5	Modular-arithmatic; Diffie-Hellman public key encryption	Handouts will be provided. Hw 4 will be assigned.	Hw 3 is due.
Week 6	Two-party secure multi-party computing; Yao's garbled circuit	Handouts will be provided.	Hw 4 is due.
Week 7	Oblivious transfer; BGW protocol	Handouts will be provided.	**Midterm Exam (tentative)**
Week 8	Zero-knowledge proofs Verifiable computing	Handouts will be provided. Hw 5 will be assigned.	
Week 9	Secure and privacy-preserving machine learning	Handouts will be provided.	Hw 5 is due. Project proposal is due.
Week 10	Coded computing	Handouts will be provided.	
Week 11	Federated learning and differential privacy	Handouts will be provided.	
Week 12	Intro to cryptography & crypto currencies	Handouts will be provided.	
Week 13	Overview of consensus protocols	Handouts will be provided.	
Week 14	Bitcoin nuts and bolts	Handouts will be provided.	
Week 15	Proof of Work and mining strategies	Handouts will be provided.	Project reports are due.
Week 16	Project presentation		

Statement on Academic Conduct and Support Systems

Academic Conduct:

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in SCampus in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on scientific misconduct, policy.usc.edu/scientific-misconduct.

Support Systems:

Student Health Counseling Services - (213) 740-7711 – 24/7 on call
engemannshc.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-4900 – 24/7 on call
engemannshc.usc.edu/rsvp
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

Office of Equity and Diversity (OED) | Title IX - (213) 740-5086
equity.usc.edu, titleix.usc.edu
Information about how to get help or help a survivor of harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants. The university prohibits discrimination or harassment based on the following protected characteristics: race, color, national origin, ancestry, religion, sex, gender, gender identity, gender expression, sexual orientation, age, physical disability, medical condition, mental disability, marital status, pregnancy, veteran status, genetic information, and any other characteristic which may be specified in applicable laws and governmental regulations.

Bias Assessment Response and Support - (213) 740-2421
studentaffairs.usc.edu/bias-assessment-response-support
Avenue to report incidents of bias, hate crimes, and microaggressions for appropriate investigation and response.

The Office of Disability Services and Programs - (213) 740-0776
dsp.usc.edu
Support and accommodations for students with disabilities. Services include assistance in providing readers/notetakers/interpreters, special accommodations for test taking needs, assistance with architectural barriers, assistive technology, and support for individual needs.

USC Support and Advocacy - (213) 821-4710
studentaffairs.usc.edu/ssa

Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity at USC - (213) 740-2101

diversity.usc.edu

Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call

dps.usc.edu, emergency.usc.edu

Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-120 – 24/7 on call

dps.usc.edu

Non-emergency assistance or information.