CS-523

Advanced topics on privacy enhancing technologies

Troncoso Carmela, Hubaux Jean-Pierre

Cursus	Sem.	Type
Computer science	MA2, MA4	Opt.
Cybersecurity	MA2, MA4	Opt.
Data Science	MA2, MA4	Opt.
SC master EPFL	MA2, MA4	Opt.

Language of teaching	English
Credits	7
Session	Summer
Semester	Spring
Exam	Written
Workload	210h
Weeks	14
Hours	**6 weekly**
Courses	3 weekly
Exercises	1 weekly
Project	2 weekly
Number of positions	

Summary

This advanced course will provide students with the knowledge to tackle the design of privacy-preserving ICT systems. Students will learn about existing technologies to protect privacy, and how to evaluate the protection they provide.

Content

The course will delve into the following topics:

- Privacy definitions and concepts, and the socioeconomic context of privacy: economics and incentives, ethics, regulation.
- Cryptographic privacy solutions: Identity management and anonymous credentials, zero-knowledge proofs, secure multi-party computation, homomorphic encryption, garbled circuits, Private information retrieval (PIR), Oblivious RAM (ORAM)
- Anonymization and data hiding: generalization, differential privacy, etc
- Machine learning and privacy: how machine learning can be use to infer private information; and how much information can be learned from machine learning models.
- Protection of metadata: anonymous communications systems, location privacy, censorpship resistance.
- Online tracking.
- Evaluation of privacy-preserving systems - notions, definitions, quantification / computation

Keywords

Privacy, anonymity, homomorphic encryption, secure multi-paty computation, anonymous credentials, ethics

Learning Prerequisites

Required courses

COM-402 Information Security and Privacy
COM-301 Computer Security

Recommended courses
COM-401 Cryptography

Important concepts to start the course
Basic programming skills; basics of probabilities and statistics; basics of cryptography

Learning Outcomes
By the end of the course, the student must be able to:
- Select appropriately privacy mechanisms
- Develop privacy technologies
- Assess / Evaluate privacy protection
- Reason about privacy concerns

Teaching methods
Lectures

Expected student activities
Participate to lectures
Do the exercises
Successfully prepare to the exam

Assessment methods
Final exam

Supervision
Assistants Yes

Resources
Bibliography
Will be provided at the first lecture