Advanced topics on Privacy Enhancing Technologies (CS-523)

Preliminaries

Carmela Troncoso

SPRING Lab

The team

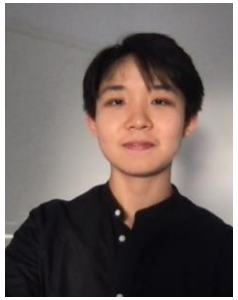
Head / Main Lecturer

Theresa Stadler
(she/her)

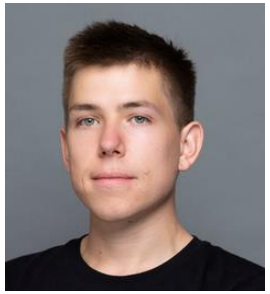
Support / Remote Lecturer

Carmela Troncoso
(she/her)

Teaching Assistants



Boya
Wang
(any pronoun)



Christian
Knabenhans
(he/him)

Neelu
Kalani
(she/her)

Malo
Perez
(he/him)

Mathilde
Raynal
(she/her)

Saiid El Hajj
Chehade
(he/him)

Shailesh
Mishra
(he/him)

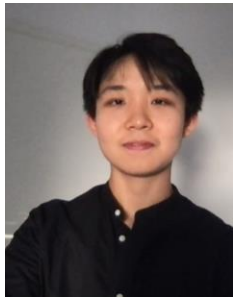
Eric
Jollès
(he/him)

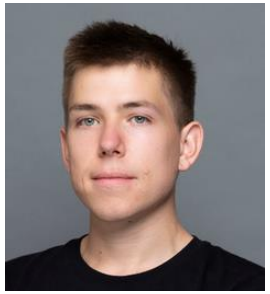
The course language(s)

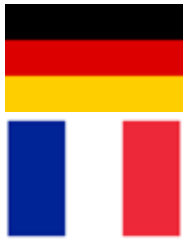
Head / Main Lecturer

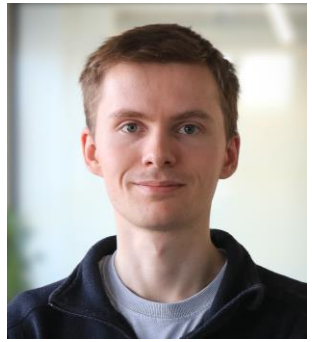
Support / Remote Lecturer

Teaching Assistants







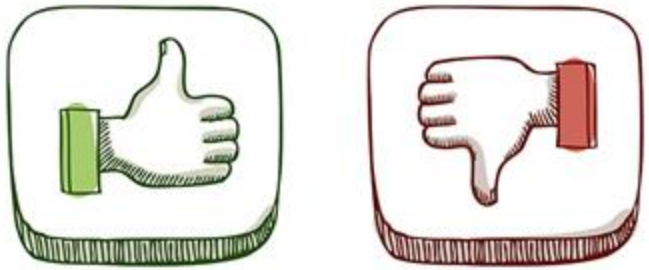


Course Aims

Course Aims

Get familiar with a number of privacy mechanisms, learn their purpose and limitations.
At the end you will have a **toolbox for privacy engineering**

Knowledge of tools and mechanisms



Evaluate pros and cons in different scenarios

Departure point for further search

Prerequisites

- COM-402 Information Security and Privacy
- COM-301 Computer Security
- Some background in cryptography will be very useful, e.g.

  COM-401 – Cryptography and security

- Light background on Machine Learning, e.g., bachelor introduction at EPFL

Topics we will cover

Attribute-based credentials

Anonymization

Differential privacy

Location privacy

Anonymous communications

Privacy engineering

Privacy-preserving cryptography

Tracking

Censorship resistance

Machine learning & privacy

Legal aspects

Themes

Attribute-based credentials CRYPTO

Anonymization DATA PUBLISHING

Differential privacy DATA PUBLISHING

Location privacy META DATA

Anonymous communications META DATA

Privacy engineering OVER ARCHING

Privacy-preserving cryptography CRYPTO

Tracking META DATA

Censorship resistance META DATA

Machine learning & privacy OVER ARCHING

Legal aspects OVER ARCHING

Layers

Attribute-based credentials APPLICATION

Anonymization APPLICATION

Differential privacy APPLICATION

Location privacy APPLICATION

Anonymous communications NETWORK

Privacy engineering ALL LAYERS

Privacy-preserving cryptography APPLICATION

Tracking APPLICATION

Censorship resistance NETWORK

Machine learning & privacy APPLICATION

Legal aspects ALL LAYERS

Schedule

		Lecture (Tuesday)	Lecturer
Week 1	Feburary, 18	Preliminaries + Intro	Troncoso
Week 2	Feburary, 25	Privacy-preserving crypto I (SMC)	Lueks
Week 3	March, 4	Privacy-preserving crypto II (Homomorphic)	Chatel
Week 4	March, 11	Privacy-preserving authentication	Raynal
Week 5	March, 18	Protecting data release I	Stadler
Week 6	March, 25	Protecting data release II	Stadler
Week 7	April, 1	Location privacy	Stadler
Week 8	April, 8	Anonymous Communications	Stadler
Week 9	April, 15	Midterm	
Week 10	April, 22	Easter break	
Week 11	April, 29	Web/Tracking	Kubicek
Week 12	May, 6	Censorship resistance	Stadler
Week 13	May, 13	Machine Learning	Cretu
Week 14	May, 20	Privacy engineering	Stadler
Week 15	May, 27	Legal aspects	Veale

Schedule

		Lecture (Tuesday)	Lecturer
Week 1	Feburary, 18	Preliminaries + Intro	Troncoso
Week 2	Feburary, 25	Privacy-preserving crypto I (SMC)	Lueks
Week 3	March, 4	Privacy-preserving crypto II (Homomorphic)	Chatel
Week 4	March, 11	Privacy-preserving authentication	Raynal
Week 5	March, 18	Protecting data release I	Stadler
Week 6	March, 25	Protecting data release II	Stadler
Week 7	April, 1	Location privacy	Stadler
Week 8	April, 8	Anonymous Communications	Stadler
Week 9	April, 15	Midterm	
Week 10	April, 22	Easter break	
Week 11	April, 29	Web/Tracking	Kubicek
Week 12	May, 6	Censorship resistance	Stadler
Week 13	May, 13	Machine Learning	Cretu
Week 14	May, 20	Privacy engineering	Stadler
Week 15	May, 27	Legal aspects	Veale

Course Organization - Activities

Live lectures (2h / week)

With Lecturer Tue 14:15-16h

Hands-on exercise solving (2h / week)

With Lecturer or TA (1h, Tue 16:15-17h)

With TAs (1h, Fri 10:15-11h)

Programming projects & Theory exercises (support 2h/week, Fri 11:15-13h)

Course Organization – Live lectures (Tuesday 14-16h)

2 x 45 minute lectures (**INF 1**) with new material

Material will be on Moodle beforehand

Questions during the lectures are encouraged!

There will be class recordings available from previous years. Not all of them are high quality, and they may deviate slightly from this years' lectures

Course Organization – Joint exercise solving (Tuesday 16-17h / Fridays 10-11h)

2 x 45 minute live exercises to apply the lecture learnings

Tuesdays with Lecturer or TA (**INF 1**), after the concepts are presented

Fridays with a TA (**INR 219** and **INM202**), drill the concepts

Exercises similar to the exam to help you develop your privacy reasoning

Strongly encourage participation: applying theory is hard, so practice!

We will NEVER record joint exercise solving. We want to encourage participation!

Course Organization – Written Exercises & Programming

Support from TAs with doubts and problems

Fridays 11:15-13h **INR 219**

Written exercises:

Exercises to help concepts from the class to sink-in

For **Programming Projects**:

Specialized TAs. Booking time required

details will follow on Moodle & on Friday's intro

Course Organization – Programming projects

Goal: put in practice the privacy techniques taught in the course
reason about privacy and implement privacy evaluations
execute your first (toy) privacy engineering project

Two projects:

Project 1: secure multi-party computation programming

Project 2: build an end-to-end privacy-preserving system

2.1. Private authentication

2.2. Private use of data

2.3. Meta data protection

Course Organization – Programming projects

Work in trios: we will let you choose your own teammates till Feb 28th. If by then you have not found teammates, write an email to cs523@groupes.epfl.ch and we will create the missing groups.

1. You **do** need a group
2. Groups are for **both** projects

Submit your group via: https://forms.gle/3LANqQrQCf2dTLef7 by Feb 28th

Assessment & Grading

- Two exams on Moodle: Midterm (15th April) and Final (TBD SAC)

- Grade: Exams + Programming Projects

```
0.15*project1_grade + 0.25*project2_grade + 0.2*midterm_grade + 0.4*exam_grade
```

- You are **never** assessed during the lectures / exercises / forum / office hours

  Participate openly and freely → Ask questions in class and outside (the earlier the better!)

  Asking and answering help exercising your **privacy-aware thinking**

Exams

- Questions about privacy technologies and principles learned in the course
  - *Including* concepts learned in the programming projects
  - No memorization, questions require reasoning

- **Closed-book written exams (cheatsheet allowed)**
- No open chat: you are not allowed to communicate/collaborate with others to do the exam (including AI assistants)
- No open copy (no plagiarism). You cannot copy text:
  - From the internet (including AI assistants)
  - From your colleagues (nor collaborate to produce text)

Exams

No, we do not publish exam answers.

No, we won't publish them even if the whole class asks

No, we won't publish them even if Anna Fontcuberta asks

Yes, it is possible to study without previous exams' answers

In fact, previous exams answers will not allow you to correct yourself

Many correct answers per question!

If you want to know how you are doing

Ask the teaching team about your answers

Ask your colleagues about your answers ← discussion is a great study technique

Sickness

Physical & mental health **are the most important**

To protect your physical health, your colleagues' and the teaching staff's please don't come to class if you are sick

We'll be available to help outside of the course: ask for student hours!

If you miss the midterm or a homework deadline due to medical reasons, talk to us. We will find a solution

Really, talk to us, but early -- we cannot change the past, but can influence the future

Code of Conduct

We expect **high integrity and professional** conduct **inside** of this course

Programming projects must be solved within the **assigned trios**
Exams must be solved **individually**

Cheating and plagiarism are **not** allowed and **will be severely penalized**

Code of Conduct

We expect **high integrity and professional** conduct **outside** of this course

- We will learn about **attacks**. We expect you to respect
  - Conventions regarding Computer Misuse and Data Protection
    - **Not acceptable** to mount attacks on live systems
    - **Not acceptable** to collect real private data
  - There are procedures for research with human subjects
  - **Responsible research** and disclosure procedures (White hat hacking)
  - Compliance and risk based assessments

If you need help

If you need somebody….

- Google is your friend (Google Scholar too!!)

- Ask us!
  - In person: on Tuesdays or Fridays or ask for student hours
  - Via Ed (**strongly preferred**: everyone learns!)
  - Via email : cs523@groupes.epfl.ch

Moodle

https://moodle.epfl.ch/course/view.php?id=15769

- Slides and live exercises for Tuesday will be available before the lecture
  - slides are **only** support material: attend classes, take notes, ask questions
- Exercises available by Tuesday before the exercise session on Friday
  - answers available on Friday after the session

Use Ed: https://edstem.org/eu/courses/1793/discussion/

- Ask early, ask often, do not suffer in silence: in class, in forum, in student hours
- Questions on the forum will **not** be considered for the grade

What now?

- Today: intro lecture
- Friday 21st: Project 1 presentation @10am in INR 219
- Friday 28th: last day to submit trios for the projects