Welcome to EPFL

Prof. Mathias Payer

Feb. 16, 2022
Welcome to the School of Computer & Communication Sciences
School of Computer and Communication Sciences - IC

- Internationally highly ranked
- 55 professors
- Internationally recognized
- Strong industrial liaison
- Core + interdisciplinary science: Collaboration with Life Sciences, Mathematics, Microengineering, Electrical Engineering, etc.
Exchange semester at EPFL

- Students:
  - Have to take courses for 20 – 35 credits.
  - Must fill in the form (ETHZ study plan) prior to the beginning of the semester at EPFL.
  - ETHZ study plan may be changed within the first two weeks of the semester. Changes must be communicated to ETHZ studies administration: bernadette.gianesi@inf.ethz.ch

- The EPFL course list for Cyber Security is available at: go.epfl.ch/MS-cybersecurity-courselist
# Important dates

[go.epfl.ch/academic-calendar](go.epfl.ch/academic-calendar)

<table>
<thead>
<tr>
<th>Deadlines – Spring 2022</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>March 4</td>
<td>Registration for spring semester courses</td>
</tr>
<tr>
<td>April 30</td>
<td>Exam-session timetable is released</td>
</tr>
<tr>
<td>May 6</td>
<td>Withdrawal from exams for spring semester</td>
</tr>
<tr>
<td>June 20-July 9</td>
<td>Summer examination session</td>
</tr>
<tr>
<td>July 29</td>
<td>Exam results are published</td>
</tr>
</tbody>
</table>

[5]
Semester project

▪ You can do the semester project here
▪ Interested students should contact the laboratories at EPFL directly.
▪ The project must be done in the field of Cyber Security.
▪ Once a project has been identified, submit the form to the EPFL admin.
▪ Register the project in IS-Academia after approval.

go.epfl.ch/IC-semester-project-procedure    go.epfl.ch/projects-cyber-labs
Internship in industry

go.epfl.ch/IC-internships

▪ Possibility to do an internship in industry through the IC network.
▪ Interested students must contact the internship office at the start of their semester.
▪ Patricia Genet can answer any questions in relation to an internship in industry.

Internship Office

Patricia Genet
Internship Program Assistant
patricia.genet@epfl.ch
Building INN - Office 131
021 693 56 41
Administrative contacts

Prof. Karl Aberer
Head of Program

Elise van Eijs
Master Program Assistant

Eileen Hazboun
Deputy Head, BS/MS Programs

Patricia Genet
Internship Program Assistant
Security and Privacy Ecosystem @ IC
Security and Privacy Classes

- COM-401 Cryptography and security (Fall)
- COM-402 Information security and privacy (Fall)
- CS-412 Software security (Spring)
- CS-438 Decentralized systems engineering (Fall)
- COM-501 Advanced cryptography (Spring)
- COM-506 Student seminar: security protocols and applications (Spring)
- CS-725 Topics in Language-based Software Security (Fall)
Techniques and abstractions for building trustworthy computer systems
(i.e., systems that are safe and secure)

- Explore the fundamental challenges posed to security and safety by large-scale systems consisting of many threads, many nodes, and millions of lines of code written by many programmers
- Solve real-world problems, overcome theoretical worst-case limitations, open-source prototypes
- Operating systems + formal methods + computer architecture
- Examples: Trustworthy network devices, Performance clarity, Secure smart-home infrastructure, …
Theoretical Computer Science and Computer Security. Specific interests include theoretical and applied cryptography, complexity theory, privacy-enhancing technologies, and quantum information.
The DEDIS team is working on projects related to large-scale collective authorities (cothorities), which distribute trust among a number of independent parties to allow scalable self-organizing communities.

With no single trusted party, cothorities can secure software updates, provide public randomness, enable privacy-conscious medical-data sharing and more.
Current research topics:

- Applied cryptography
- Secure, federated analytics
- Protection of health data

Because of Prof. Hubaux’s retirement from professorial activities, the LDS lab will be closed in summer 2022.

6 former members of the lab have joined spin-off Tune Insight on January 1st, 2022. The company is looking for interns; contact: juan@tuneinsight.com.

At EPFL, Prof. Hubaux will continue working for C4DT.org, EPFL’s interface to the external world on the topic of digital trust.

LDS will not be able to host additional semester projects.

https://lds.epfl.ch
Security and Privacy Engineering Lab (SPRING)

- Analyze, build, and deploy secure and privacy-preserving systems
- Collaborate with real-world partners
- Apply crypto to build systems in new ways
- Reason about security and privacy of Machine learning

- Semester Projects
- PhD

Carmela Troncoso carmela.troncoso@epfl.ch
https://spring.epfl.ch/
Software Testing
- Goal: prune bugs
- Helps developers
- Fuzzing discovers them
- Sanitization detects them

Mitigations
- Goal: stop exploitation
- Last line of defense
- Guard control flow (CFI)
- Type-aware data guards

Compartments
- Goal: fail safe
- Small, safe components
- ISA abstractions
- Kernel extensions
Design **concurrent and safe** systems software: OSes, storage stack, and data processing systems

**Scalability:** Scale OS operations with increasing core count

**Robustness:** Remove vulnerabilities from existing OSes

Ex: Formally verified concurrent OS, Undo OS, fuzzing distributed storage stack, scalable trusted execution environments

Sanidhya Kashyap
https://rs3lab.github.io
The Security and Cryptography Laboratory (LASEC) was created at EPFL in 2000. It is part of the School of Computer and Communication Sciences (I&C). The main activities of LASEC are research and education on the security of communication and information systems, cryptography, and applications.
What are you interested on? Talk to us!

Networks
- NAL
- Argyraki

Distributed Systems
- DEDIS
- Ford
- DCL
- Guerraoui
- SaCS
- Kermarrec

Crypto
- LASEC
- Vaudenay
- COMPSEC
- Chiesa

Hardware Security
- PARS
- A
- Falsafi

Systems Security
- DSLab
- HexHive
- Candea
- Payer
- RS3Lab
- Kashyap

Privacy
- SPRING
- Troncoso
- LDS
- Hubaux

Machine Learning
- TML
- Flammarion
- MLO
- Jaggi
Capture The Flag (CTF)

- A cybersecurity competition
- Often involving real-world attacks
- You score points by capturing the flag of a given challenge
- The flag is a secret/hidden string
- https://polygl0ts.ch/
We wish you an excellent semester!

Any Questions?