Welcome to EPFL

Prof. Mathias Payer

Feb. 23, 2023
Welcome to the School of Computer & Communication Sciences
School of Computer and Communication Sciences - IC

- Internationally highly ranked
- 52 professors/labs
- Internationally highly recognized
- Strong industry liaison
- Core + interdisciplinary science: Collaboration with Life Sciences, Mathematics, Microengineering, Electrical Engineering, etc.
- Doctoral school
• 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

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 3</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 5</td>
<td>Withdrawal from exams for spring semester</td>
</tr>
<tr>
<td>June 19-July 8</td>
<td>Summer examination session</td>
</tr>
<tr>
<td>July 28</td>
<td>Exam results are published</td>
</tr>
</tbody>
</table>
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 from the list has been identified, register it in IS-Academia.
- If the project is off list, send the abstract and the lab’s name to EPFL Master Cyber admin for approval.
- Registration deadline in IS-Academia = 3rd March 2023

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.

Patricia Genet
Internship Program Coordinator
patricia.genet@epfl.ch
Building INN - Office 131
021 693 56 41
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.
Dependable Systems Lab

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, …

George Candea
https://dslab.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
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.
PARSA (FALSAFI)

Future-proofing memory protection
- Keeps POSIX (VMA) interface to apps
  - Linux, MacOS/iOS, Android
- Eliminates page-based translation
  ✓ Unclogs virtual memory for security, virtualization, accelerators
FPGA Security (PARSA, Stojilovic)

- Hardware security challenges of FPGA multitenancy in datacenters and the cloud
  - FPGA power viruses for transient fault injection
  - Stealthy sensors for remote power side-channel attacks

- Ongoing research
  - CPU-to-FPGA attacks targeting Ubuntu
  - Preventing attacks, bitstream scanning
  - Active fencing: hiding side-channel leakage

- Research-oriented semester projects (challenging but often rewarding)
  - E.g., cyber MSc thesis on stealthy sensors (David Spielmann, ETHZ) accepted for TCHES’23
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
- 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/
Center for Digital Trust

- **Competence center**
  - Privacy protection & cryptography, blockchains and smart contracts, software verification, device and system security, machine learning

- **Stakeholders**
  - EPFL laboratories, industrial partners, authorities

- **Activities**
  - Bilateral projects, events, workgroups & workshops, publications

- **Collaborations**
  - Swiss Support Center for Cybersecurity, CyberPeace Institute, Capital Market Technology Association, Trust Valley, international academic centers
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-523 Advanced topics on privacy enhancing technologies (Spring)
- CS-725 Topics in Language-based Software Security (Fall)
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
- PARSA Falsafi

Systems Security
- DS Lab
- HexHive
- Candea
- Payer
- RS3 Lab
- Kashyap

Privacy
- SPRING
- Troncoso

Machine Learning
- TML Flammarion
- MLO Jaggi
- DCL Guerraoui
- SaCS Kermarrec
- DEDIS Ford
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/
Your administrative contacts at EPFL

Eileen Hazboun
Deputy head
eileen.hazboun@epfl.ch
Building INN - Office 130
021 693 60 48

Antonella Veltro
Administrative specialist
antonella.veltro@epfl.ch
Building INN - Office 111
021 693 76 66
We wish you an excellent semester!