Welcome to EPFL

Prof. Mathias Payer

Feb. 19, 2024
School of Computer and Communication Sciences - IC

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

- 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: brigitteregula.marti@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>Deadlines – Spring 2024 semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 1</td>
</tr>
<tr>
<td>April 30</td>
</tr>
<tr>
<td>May 3</td>
</tr>
<tr>
<td>June 17- July 6</td>
</tr>
<tr>
<td>July 26</td>
</tr>
</tbody>
</table>
You can do the research 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 = 1st March 2024

---

### IC School of Computer and Communication Sciences IC

<table>
<thead>
<tr>
<th>URL Projects</th>
<th>Laboratory</th>
<th>Authorized supervisors</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPSEC</td>
<td>Laboratory for Computation Security</td>
<td>Prof. Alessandro Chiappa</td>
</tr>
<tr>
<td>DCL</td>
<td>Distributed Computing Laboratory</td>
<td>Prof. Rachid Guerraoui</td>
</tr>
<tr>
<td>DCIS</td>
<td>Data Center Systems Laboratory</td>
<td>Prof. Edouard Bugnon</td>
</tr>
<tr>
<td>DEDIS</td>
<td>Decentralized and Distributed Systems Lab</td>
<td>Prof. Bryan Ford</td>
</tr>
<tr>
<td>DLAR</td>
<td>Dependable Systems Laboratory</td>
<td>Prof. George Candaia</td>
</tr>
<tr>
<td>HEDSHEVE</td>
<td>Hedhve Laboratory</td>
<td>Prof. Mathias Payer</td>
</tr>
<tr>
<td>LASER</td>
<td>Security and Cryptography Laboratory</td>
<td>Prof. Serge Vaudenay</td>
</tr>
<tr>
<td>LA-CYBER</td>
<td>Artificial Intelligence Laboratory</td>
<td>Prof. Boi Feltins</td>
</tr>
<tr>
<td>LISR</td>
<td>Distributed Information Systems Laboratory</td>
<td>Prof. Karl Aberer</td>
</tr>
<tr>
<td>ML</td>
<td>Mathematics of Information Laboratory</td>
<td>Prof. Yarina Shiel</td>
</tr>
<tr>
<td>NAL</td>
<td>Network Architecture Laboratory</td>
<td>Prof. Katarina Avgnati</td>
</tr>
<tr>
<td>PARSA</td>
<td>Parallel Systems Architecture Laboratory</td>
<td>Prof. Babak Falsafi, Dr. Mirjana Stojilovic</td>
</tr>
<tr>
<td>RESE</td>
<td>Robust Scalable Systems Software Lab</td>
<td>Prof. Sandhya Kashyap</td>
</tr>
<tr>
<td>SACC</td>
<td>Scalable Computing Systems Laboratory</td>
<td>Prof. Anne-Marie Kermarec</td>
</tr>
<tr>
<td>SPRING</td>
<td>Security and Privacy Engineering Laboratory</td>
<td>Prof. Carmela Gonzalez Troncossi</td>
</tr>
<tr>
<td>SPITIME</td>
<td>Systems and Formalisms Lab</td>
<td>Prof. Clement H-Claudel</td>
</tr>
<tr>
<td>VCA</td>
<td>Verification and Computer Architecture Lab</td>
<td>Prof. Thomas Bourgeois</td>
</tr>
<tr>
<td>STI School of Engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIS</td>
<td>Laboratory of Intelligent Systems</td>
<td>Prof. Dario Fioreano</td>
</tr>
</tbody>
</table>

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

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
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
COMPSEC

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.
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, …
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
LASEC

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
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

- Research 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
Our 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-510 Topics in Language-based Software Security (Fall)
What are you interested on? Talk to us!

- Networks
  - NAL
  - Argyraki

- Distributed Systems
  - DEDIS
  - Ford
  - DCL
  - Guerraoui

- 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
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

Jasmine Locatelli
Administrative specialist
jasmine.locatelli@epfl.ch
Building INN - Office 112
021 693 28 50
We wish you an excellent semester!

Any Questions?

Hack the planet!