



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

Deadlines – Spring 2022

March 4	Registration for spring semester courses
April 30	Exam-session timetable is released
May 6	Withdrawal from exams for spring semester
June 20-July 9	Summer examination session
July 29	Exam results are published

EPFL Semester project

6

- 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

URL Projects	Laboratory	Authorised supervisors
IC School of Computer and Communication Sciences IC		
<u>COMPSEC</u>	Laboratory for Computation Security	Prof. Alessandro Chiesa
<u>DCL</u>	Distributed Computing Laboratory	Prof. Rachid Guerraoui
<u>DCSL</u>	Data Center Systems Laboratory	Prof. Edouard Bugnion
<u>DEDIS</u>	Decentralized and Distributed Systems Lab	Prof. Bryan Ford
<u>DSLAB</u>	Dependable Systems Laboratory	Prof. George Candea
<u>HEXHIVE</u>	HexHive Laboratory	Prof. Mathias Payer
<u>LASEC</u>	Security and Cryptography Laboratory	Prof. Serge Vaudenay
<u>LDS</u>	Laboratory for Data Security	Prof. Jean-Pierre Hubaux
<u>LIA</u>	Artificial Intelligence Laboratory	Prof. Boi Faltings
<u>LSIR</u>	Distributed Information Systems Laboratory	Prof. Karl Aberer
<u>NAL</u>	Network Architecture Laboratory	Prof. Katerina Argyraki
<u>PARSA</u>	Parallel Systems Architecture Laboratory	Prof. Babak Falsafi
<u>PARSA BIS</u>	PARSA BIS	Dr. Mirjana Stojilovic
<u>SPRING</u>	Security and Privacy Engineering Laboratory	Prof. Carmela Gonzalez Troncoso

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

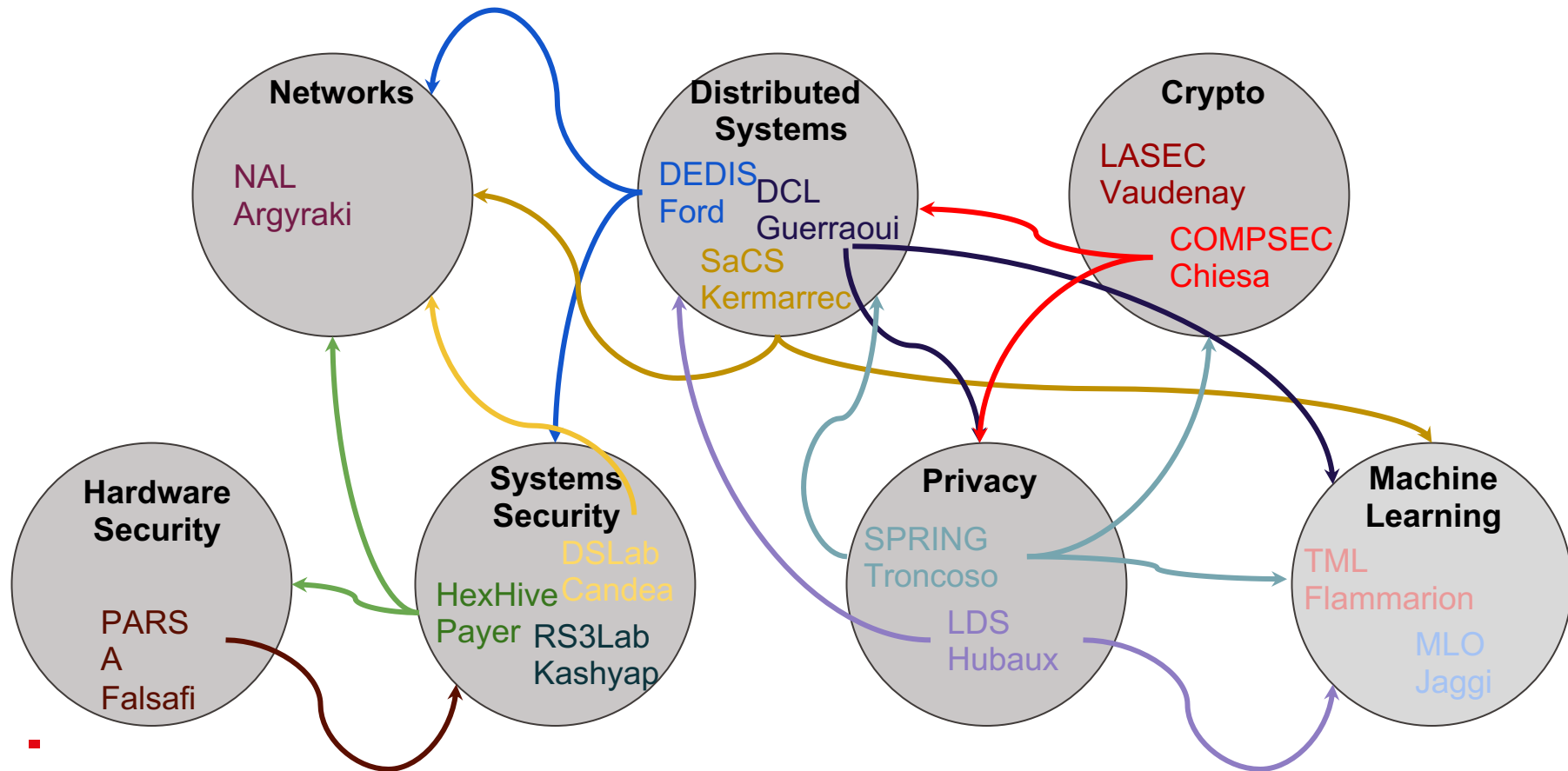
Deputy Head, BS/MS Programs



Patricia Genet

Internship Program Assistant

EPFL 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, ...



George Candea
<https://dslab.epfl.ch>

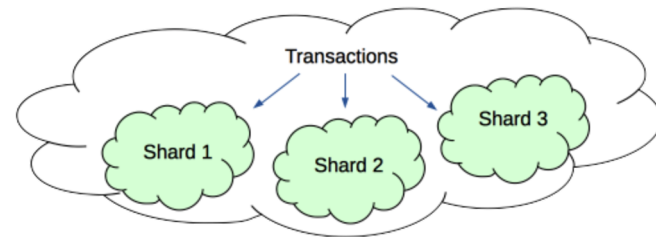


Theoretical Computer Science and Computer Security. Specific interests include theoretical and applied cryptography, complexity theory, privacy-enhancing technologies, and quantum information.



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.



<u>Alp, Enis Ceyhun</u>	Doctoral Assistant
<u>Basescu, Cristina</u>	Doctoral Assistant
<u>Borsò, Pierluca</u>	Computer Scientist
<u>Colombo, Simone</u>	Doctoral Assistant
<u>Estrada-Galiñanes, Vero</u>	Scientist
<u>Ford, Bryan Alexander</u>	Associate Professor
<u>Hünsch, Sandra Renata</u>	Administrative Assistant
<u>Kocher, Noémien</u>	Computer Scientist
<u>Lopes, Yves</u>	Systems Engineer
<u>Lüthi, Marc-André</u>	ETS/HES Engineer
<u>Merino, Louis-Henri Manuel Jakob</u>	Doctoral Assistant
<u>Nikitin, Kirill</u>	
<u>Subira Nieto, Jordi</u>	Student/Auxiliary
<u>Tennage, Pasindu Nivanthaka</u>	Doctoral Assistant
<u>Viaene, Jean</u>	Computer Scientist
<u>Zhang, Haoqian</u>	Doctoral Assistant

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>



EPFL 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>





- 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

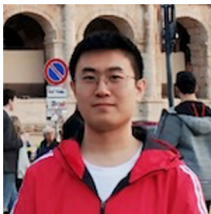


Robustness: Remove vulnerabilities from existing OSes

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.

Prof. Serge Vaudenay  

Martine Corval 

Senior Researchers

Subhadeep Banik  

Thomas Lochmatter  

Researchers

Khashayar Barooti  

Andrea Caforio  


Daniel Collins  



Loïs Huguenin 


Aymeric Genet 

Novak Kaluderovic  

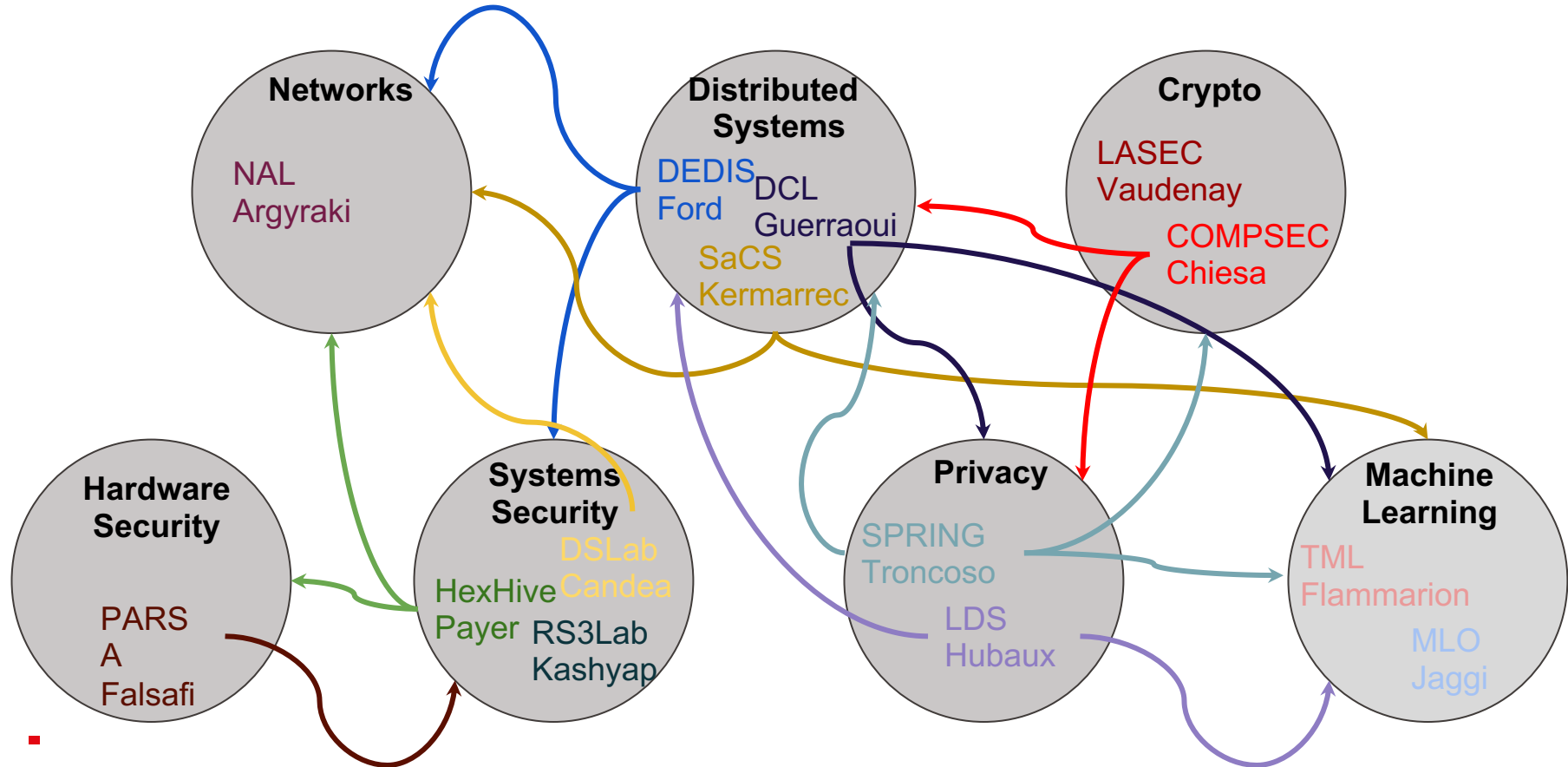
Laurane Marco 

Dalia Papuc 

Abdullah Talayhan  

Bénédikt Tran 

EPFL What are you interested on? Talk to us!



EPFL 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?