ESORICS 2025

30th European Symposium on Research in Computer Security

September 22-26, 2025

Toulouse, France

IRIT

LAAS CNRS

Défis Clés OCCITANIE

La Région Occitanie Pyrénées · Méditerranée

ICO Institut Cybersécurité Occitanie

Université de Toulouse

cnrs

Photo cover : © Gaël Fontaine

Preface

On behalf of the Organization Committee of the 30th European Symposium on Research in Computer Security (ESORICS2025), it is our pleasure to welcome you to Toulouse, France.

ESORICS was founded to further the progress of research in computer, information and cyber security and in privacy, by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

Since its inception in 1990, ESORICS has been hosted in a series of European countries and has established itself as the premiere European research event in computer security. Starting biannually in 1990 in Toulouse, the symposium has been held annually since 2002. We are delighted to welcome you to the 30th edition of the symposium in Toulouse, where it was first held.

As one of the longest-running reputable conferences focused on security research, ESORICS 2025 attracted numerous high-quality submissions from all over the world, with authors affiliated with diverse academic, non-profit, governmental, and industrial entities. After two rounds of submissions, each followed by an extensive reviewing period, we wound up with an excellent program, covering a broad range of timely and interesting topics. A total of 605 unique submissions were received: 150 in the first round and 475 in the second (of which 20 were invited resubmissions.) The international Program Committee (204 members from 47 countries), selected 100 of them for presentation and for publication in the ESORICS 2025 Proceedings in the Springer LNCS Series (LNCS 16053, 16054, 16055, 16056).

The program is enriched by keynotes given by renowned speakers: «Out of sight, out of mind: the plumbing problem in Cybersecurity» by Carlos Aguilar, «Covert Social Influence Operations: Past, Present, and Future» by V.S. Subrahmanian; and «Data Privacy and Security in Distributed Collaborative Scenarios», by Pierangela Samarati.

The conference is organized in a three parallel tracks conference, allowing intensive networking during breaks and social events, and participation in all presentations and discussions. For this edition, we had 13 high-quality workshops after the main conference, on Thursday and Friday: ANUBIS, AutoCyber, CBT, CPS4CIP, CyberICPS, DISA, DPM, HS3, MIST, SECAI, SecAssure, STM and STMUS. These workshops differ according to the topic, goals and organizing group(s), and are published in separate ESORICS Workshop Proceedings (LNCS 16231, 16232, 16233).

We would like to express our gratitude and thanks to all those who contributed to make this conference possible: the authors of submitted papers and the invited speakers; the Program Committee members and the external reviewers; and last but not least the Local Organization Committee and particularly members of University of Toulouse, of LAAS and IRIT labs, as well as members of the Institute for Cybersecurity in Occitanie (ICO), who took care of the local arrangements.

Thank you for attending the conference. We hope that you will benefit from the conference and that you will find our efforts worthwhile. We wish you a pleasant stay in Toulouse. Enjoy!

Abdelmalek Benzekri,
General Chair

Vincent Nicomette,
General Chair

Conference Program

Overview

	September 22		
From 08:00	Registration		
8:45 - 9:00	**Welcome statement**		
9:00 - 10:00	**Keynote :Carlos Aguilar** (*SandBoxAQ, France*)		
10:00 - 10:20	Coffee Break		
10:20 - 12:00	**Track 1** *Privacy 1*	**Track 2** *Attack Analysis 1*	**Track 3** *Crypto 1*
12:00 - 13:30	Lunch		
13:30 - 15:10	**Track 4** *Privacy 2*	**Track 5** *Detection 1*	**Track 6** *Crypto 2*
15:10 - 15:40	Coffee Break		
15:40 - 17:20	**Track 7** *Attack Analysis 2*	**Track 8** *Privacy 3*	**Track 9** *Crypto 3*
17:20 - 17:30	Conference Information		
18:30	Welcome Reception at the City-Hall of Toulouse Please note that a security check will be carried out at the entrance to the city hall. Unauthorized items will be thrown away (sharp objects, flammable pro-ducts, water bottles, etc.).		

	September 23		
8:30 - 9:00	Registration		
9:00 - 10:00	**Keynote : V.S. Subrahmanian** (*Northwestern University, USA*)		
10:00 - 10:30	Coffee Break		
10:30 - 12:10	**Track 10** *Blockchain Secured Systems*	**Track 11** *Vulnerability Assessment*	**Track 12** *Crypto 4*
12:10 - 14:00	Lunch		
14:00 - 15:40	**Track 13** *AI Security 1*	**Track 14** *Detection 2*	**Track 15** *Mitigation*
15:40 - 16:10	Coffee Break		
16:10 - 17:50	**Track 16** *AI security 2*	**Track 17** *Protection*	**Track 18** *Attack Analysis 3*
17:50 - 18:00	Conference Information		
19:30	Gala Dinner at Hotel Dieu		

September 24			
08:30 - 9:00	Registration		
9:00 - 10:00	**Keynote : Pierangela Samarati** *(Universita degli Studi di Milano, Italia)*		
10:00 - 10:30	Coffee Break		
10:30 - 12:10	**Track 19** *Security Protocols 1*	**Track 20** *Access and Information Flow Control*	**Track 21** *Security Protocols 2*
12:10 - 14:00	Lunch		
14:00 - 15:15	**Track 22** *Software Testing 2*	**Track 23** *Software Testing 1*	**Track 24** *Attack Analysis 4*
15:15 - 15:45	Coffee Break		
15:45 - 17:00	**Track 25** *Post-Quantum*	**Track 26** *AI Security 3*	**Track 27** *Privacy 4*
17:00 -17:20	Conference Closing Remarks (awards, annoucements and workshops information)		

Workshop Program

Overview

Day	Hour	Concorde (Bât. U4)	Apmhi Schwartz (Bât. IMT)	Amphi J. Herbrant (IRIT)	Amphi Condat (Main Building)	Thesis Room (IRIT)	Meeting Room (Bât. U3)	Room 01 (IRIT)
Thursday	09h00-10h30	AutonomousCyber	CPS4CIP	CyberICPS	DPM	HS3	CBT	DiSA
	10h30-10h50	Coffee break (Main Building)						
	10h50-12h20	AutonomousCyber	CPS4CIP	CyberICPS	DPM	HS3	CBT	STMUS
	12h20-13h50	Lunch Break (Main Building)						
	13h50-15h20	STM	SECAI	CyberICPS	DPM	HS3	CBT	STMUS
	15h20-15h40	Coffee break (Main Building)						
	15h40-17h10	STM	SECAI	CyberICPS	DPM	HS3	CBT	STMUS
	19h	Workshops Dinner						
Friday	09h00-10h30	STM	SECAI	ANUBIS		MIST	SecASsure	
	10h30-10h50	Coffee break (IRIT)						
	10h50-12h20	STM	SECAI	ANUBIS		MIST	SecASsure	
	12h20-13h50	Lunch Break (Main Building)						
	13h50-15h20	STM	SECAI	ANUBIS		MIST	SecASsure	
	15h20-15h40	Coffee break (IRIT)						
	15h40-17h10	STM	SECAI	ANUBIS		MIST	SecASsure	

Commitees

Steering Committee

Joachim Biskup
Frederic Cuppens
Sabrina De Capitani di Vimercati
Joaquin Garcia-Alfaro (chair)
Dieter Gollmann
Sushil Jajodia
Sokratis Katsikas
Mirek Kutylowski
Javier Lopez
Jean-Jacques Quisquater
Peter Y A Ryan
Pierangela Samarati
Einar Snekkenes
Michael Waidner
Edgar Weippl

General Chairs

Vincent Nicomette (LAAS-CNRS, INSA de Toulouse)
Abdelmalek Benzekri (IRIT, Université de Toulouse)

Program Chairs

Nora Boulahia-Cuppens (Polytechnique Montréal)
Jaideep Vaidya (Rutgers University)

Publicity Chairs

Paria Shirani (University of Ottawa, Canada)
Wenjuan Li (The Education University of Hong Kong, China)
Sebastien Bardin (Software Safety and Security Lab, CEA, France)

Organization Chairs

Denise Gross (ICO)
Justine Praneuf (LAAS-CNRS)
Charlotte Sébastien (Université de Toulouse)
Tifanny Vest (Université de Toulouse)

Workshops Chair

Romain Laborde (IRIT, Université de Toulouse)

Sponsor Chair

Giorgia Macilotti (Airbus Protect)

Web chairs

Charlotte Sébastien (Université de Toulouse)
Tifanny Vest (Université de Toulouse)

Program Committee

Andrea Agioll (Round 2), TU Delft, The Netherlands
Massimiliano Albanese, George Mason University, USA
Cristina Alcaraz, University of Malaga, Spain
Abdelrahaman Aly, Technology Innovation Institute, United Arab Emirates
Shengwei An (Round 2), Virginia Tech, USA
Hafiz Asif (Round 2), Hofstra University, Rutgers University, USA
Mikael Asplund, Linköping University, Sweden
Vijay Atluri, Rutgers University, USA
Daniel Augot (Round 1), INRIA Saclay, France
Samiha Ayed (Round 2), UTT - Université des technologies de Troyes, France
Sebastien Bardin, CEA LIST, France
Alessandro Barenghi, Politecnico di Milano, Italy
Ken Barker (Round 1), University of Calgary, Canada
Giampaolo Bella (Round 2), University of Catania, Italy
Abdelmalek Benzekri, Université de Toulouse, France
Elisa Bertino, Purdue University, USA
Clara Bertolissi (Round 2), Aix-Marseille University, France
Bruhadeshwar Bezawada (Round 2), Southern Arkansas University, USA
Smriti Bhatt (Round 2), Purdue University, USA
Giuseppe Bianchi (Round 2), University of Rome "Tor Vergata", Italy
Alex Biryukov, University of Luxembourg, Luxembourg
Jorge Blasco (Round 1), Universidad Politécnica de Madrid, Spain
Carlo Blundo, Università degli Studi di Salerno, Italy
Tamara Bonaci (Round 2), Northeastern University, USA
Rainer Böhme (Round 2), University of Innsbruck, Austria
Pino Caballero-Gil, University of La Laguna, Spain
Maurantonio Caprolu (Round 2), King Abdullah University of Science and Technology, Saudi Arabia
Xavier Carpent, University of Nottingham, UK
Aldar C-F. Chan (Round 2), University of Hong Kong, China
Bo Chen (Round 2), Michigan Technological University, USA
Rongmao Chen (Round 2), National University of Defense Technology, China
Xiaofeng Chen (Round 2), Xidian University, China
Yuan Cheng (Round 2), University of Nottingham Ningbo China, China
Sherman S. M. Chow (Round 2), The Chinese University of Hong Kong, China
Pietro Colombo (Round 2), Università dell'Insubria, Italy
Michal Choras (Round 1), Bydgoszcz University of Science and Technology, Poland
Mauro Conti, Padova University, Italy
Bruno Crispo (Round 2), University of Trento, Italy
Michel Cukier (Round 2), University of Maryland, USA
Frédéric Cuppens, Polytechnique Montréal, Canada
Tooska Dargahi, Manchester Metropolitan University, UK
Saptarshi Das (Round 2), Pennsylvania State University, USA
Sabrina De Capitani di Vimercati, Universita' degli Studi Di Milano, Italy
Hervé Debar, Télécom SudParis, France
Jose Maria De Fuentes (Round 1), Universidad Carlos III, Spain
Soumyadeep Dey (Round 2), IIT Kharagpur, India
Roberto Di Pietro (Round 2), King Abdullah University of Science and Technology, Saudi Arabia
Tassos Dimitriou (Round 2), Kuwait University, Kuwait
Xuhua Ding (Round 1), Singapore Management University, Singapore
Josep Domingo-Ferrer, Universitat Rovira i Virgili, Spain
Andreas Ekelhart (Round 1), Secure Business Austria, Austria
Santiago Escobar (Round 2), Universitat Politècnica de València, Spain
David Espes (Round 2), UBO - Université de Bretagne Ouest, France
Shuya Feng (Round 2), University of Connecticut, USA
Anna Lisa Ferrara, Unversità degli studi del Molise, Italy
Josep Lluís Ferrer Gomila (Round 2), Universitat de les Illes Balears, Spain
Philip W. L. Fong (Round 2), University of Calgary, Canada
Olga Gadyatskaya, University of Leiden, The Netherlands
Debin Gao, Singapore Management University, Singapore
Joaquin Garcia-Alfaro, Institut Polytechnique de Paris, France
Essam Ghadafi, Newcastle University, UK
Giorgio Giacinto, University of Cagliari, Italy
Alberto Giaretta (Round 1), Örebro Universitet, Sweden
Dieter Gollmann, Hamburg University of Technology, Germany
Lorena González Manzano, Universidad Carlos III de Madrid, Spain
Dimitris Gritzalis (Round 1), Athens University of Economics & Business, Greece
Stefanos Gritzalis (Round 2), University of Piraeus, Greece

Maanak Gupta (Round 2), Tennessee Tech University, USA
M. Emre Gursoy (Round 2), Koç University, Turkey
Gregory Gutin (Round 2), Royal Holloway, University of London, UK
Hannes Hartenstein (Round 2), Karlsruhe Institute of Technology, Germany
Hongxin Hu (Round 2), University at Buffalo, SUNY, USA
Xinyi Huang (Round 2), Fujian Normal University, Japan
Hugo Jonker, Open University of the Netherlands, The Netherlands
Sokratis Katsikas, Norwegian University of Science and Technology, Norway
Stefan Katzenbeisser, University of Passau, Germany
Jörg Keller, FernUniversität in Hagen, Germany
Latifur Khan (Round 2), University of Texas at Dallas, USA
Hiroaki Kikuchi, Meiji University, Japan
Hyoungshick Kim (Round 2), Sungkyunkwan University, South Korea
Ram Krishnan (Round 2), University of Texas at San Antonio, USA
Marina Krotofil, Maersk, Switzerland
Christopher Kruegel (Round 2), University of California Santa Barbara, USA
Alptekin Küpçü, Koç University, Turkey
Romain Laborde, Université de Toulouse, France
Peeter Laud, Cybernetica AS, Estonia
Maryline Laurent, Télécom SudParis, France
Zeyu Lei (Round 2), Purdue University, USA
Shujun Li (Round 2), University of Kent, UK
Wenting Li (Round 2), Peking University, China
Jun Li (Round 2), University of Oregon, USA
Kaitai Liang, Delft University of Technology, The Netherlands
Hoon Wei Lim (Round 2), NCS Group, Singapore
Dan Lin (Round 2), Vanderbilt University, USA
Peng Liu (Round 2), The Pennsylvania State University, USA
Giovanni Livraga, University of Milan, Italy
Valeria Loscri, INRIA, France
Wenjing Lou (Round 2), Virginia Tech, USA
Rongxing Lu (Round 2), Queen's University, Canada
Haibing Lu (Round 2), Santa Clara University, USA
Xiapu Luo (Round 2), The Hong Kong Polytechnic University, China
Eduard Marin, Telefonica Research, Spain
Jean-Yves Marion, Université de Lorraine, France
Fabio Martinelli (Round 2), IIT-CNR, Italy
Amir Masoumzadeh (Round 2), University at Albany - SUNY, USA
Barbara Masucci, University of Salerno, Italy
Wojciech Mazurczyk, Warsaw University of Technology, Poland
David Megías, Universitat Oberta de Catalunya, Spain
Weizhi Meng, Lancaster University, UK
Donika Mirdita (Round 2), Fraunhofer Secure Information Technology, Germany
Chris Mitchell (Round 2), Royal Holloway, University of London, UK
Barsha Mitra (Round 2), BITS Pilani Hyderabad Campus, India
Sudip Mittal (Round 2), Mississippi State University, USA
Meisam Mohammady (Round 2), Iowa State University, USA
Haralambos Mouratidis (Round 2), University of Essex, UK
Guillermo Navarro-Arribas, Autonomous University of Barcelona, Spain
Jianting Ning (Round 2), Singapore Management University, Singapore
Antonino Nocera, University of Pavia, Italy
Gabriele Oligeri, Hamad Bin Khalifa University, Qatar
Melek Önen (Round 2), EURECOM, France
Philippe Owezarski, LAAS-CNRS, France
Balaji Palanisamy (Round 2), University of Pittsburgh, USA
Stefano Paraboschi (Round 2), Universita di Bergamo, Italy
Sikhar Patranabis (Round 2), IBM Research India, India
Günther Pernul (Round 2), Universität Regensburg, Germany
Josef Pieprzyk, CSIRO/Data61, Australia
Joachim Posegga, Univ. of Passau, Germany
Mir Mehedi Pritom (Round 2), Tennessee Tech University, USA
Megha Quamara (Round 2), King's College London, UK
Silvio Ranise (Round 2), University of Trento, Italy
Kai Rannenberg (Round 2), Goethe University Frankfurt, Germany
Siddharth Prakash Rao (Round 2), Nokia Bell Labs, Finland
Danda B. Rawat (Round 2), Howard University, USA
Indrakshi Ray (Round 1), Colorado State University, USA
Indrajit Ray (Round 2), Colorado State University, USA
Peter Roenne, University of Luxembourg, Luxembourg
Carlos Rubio Medrano (Round 2), Texas A&M University, USA

Peter Y A Ryan, University of Luxembourg, Luxembourg
Reihaneh Safavi-Naini, University of Calgary, Canada
Pierangela Samarati, Universita' degli Studi di Milano, Italy
Neetesh Saxena, Cardiff University, UK
Neta Schiff (Round 2), Rozen Hebrew University of Jerusalem, Israel
Dominique Schröder, Universiät Erlangen-Nürnberg, Germany
Joerg Schwenk, Ruhr-Universität Bochum, Germany
Savio Sciancalepore, Eindhoven University of Technology, The Netherlands
R Sekar Stony (Round 2), Brook University, USA
Basit Shafiq (Round 2), Lahore University of Management Sciences, Pakistan
Ankit Shah (Round 2), Indiana University, USA
Siamak Shahandashti, University of York, UK
Alessandro Sorniotti (Round 1), IBM Research Europe, Switzerland
Shantanu Sharma (Round 2), New Jersey Institute of Technology, USA
Wenbo Shen (Round 2), Zhejiang University, China
Weidong Shi (Round 2), University of Houston, USA
Arunesh Sinha (Round 2), Rutgers University, USA
Jayesh Soni (Round 2), Florida International University, USA
Angelo Spognardi, Sapienza Università di Roma, Italy
Riccardo Spolaor, Shandong University, China
Natalia Stakhanova (Round 2), University of Saskatchewan, Canada
Thorsten Strufe (Round 2), Karlsruhe Institute of Technology, Germany
Wenhai Sun (Round 2), Purdue University, USA
Shamik Sural (Round 2), Indian Institute of Technology Kharagpur, India
Luis Suárez (Round 2), Ericsson, Canada
Qiang Tang (Round 2), University of Sydney, Australia
Nadia Tawbi, Laval University, Canada
Vicenc Torra, Umeå University, Sweden
Jacob Torrey (Round 2), Thinkst Applied Research, USA
Ari Trachtenberg (Round 2), Boston University, USA
Stacey Truex (Round 2), Denison University, USA
Jalaj Upadhyay (Round 2), Johns Hopkins University, USA
Tobias Urban (Round 2), Westphalian University of Applied Sciences, Germany
Daniele Venturi, Sapienza University of Rome, Italy
Rakesh Verma (Round 2), University of Houston, USA
Tran Viet Xuan Phuong (Round 2), University of Arkansas at Little Rock, USA
Joao P. Vilela (Round 2), University of Porto, Portugal,
Di Wang (Round 2), State University of New York at Buffalo, USA
Haining Wang (Round 2), Virginia Tech, USA
Cong Wang (Round 2), City University of Hong Kong, China
Xinyue Wang (Round 2), Renmin University of China, China
Lingyu Wang (Round 2), Concordia University, Canada
Han Wang (Round 2), University of Kansas, USA
Wenqi Wei (Round 2), Fordham University, USA
Edgar Weippl, University of Vienna, Austria
Avishai Wool (Round 1), Tel Aviv University, Israel
Christos Xenakis (Round 2), University of Piraeus, Greece
Yang Xiang (Round 2), Swinburne University of Technology, Australia
Yue Xiao (Round 2), IBM Research, USA
Shouhuai Xu (Round 2), University of Colorado Colorado Springs, USA
Runhua Xu (Round 2), Beihang University, China
Peng Xu (Round 2), Huazhong University of Science and Technology, China
Guomin Yang (Round 2), Singapore Management University, Singapore
Zhihao Yao (Round 2), New Jersey Institute of Technology, USA
Roland Yap (Round 2), National University of Singapore, Singapore
Miuyin Yong Wong (Round 2), Georgia Institute of Technology, USA
Chuan Yue (Round 2), Colorado School of Mines, USA
Stefano Zanero (Round 1), Politecnico di Milano, Italy
Yuan Zhang (Round 2), Fudan University, China
Zhikun Zhang (Round 2), Zhejiang University, China
Kehuan Zhang (Round 2), The Chinese University of Hong Kong, China
Liang Zhao (Round 2), Emory University, USA
Ziming Zhao (Round 2), Northeastern University, USA
Yunlei Zhao (Round 2), Fudan University, China
Jianying Zhou (Round 2), Singapore University of Technology and Design, Singapore
Sencun Zhu (Round 2), The Pennsylvania State University, USA
Rui Zhu (Round 2), Indiana University, USA

Conference Program

Monday, September 22, 2025

From 08:00		Registration / Welcome Coffee - Main Building
8:45 - 9:00		Welcome Statement - Main Building
9:00 - 10:00	Auditorium Marthe Condat	**Keynote 1 : «Out of sight, out of mind: the plumbing problem in Cybersecurity», Carlos Aguilar, SandBoxAQ -** Session Chair : Vincent Nicomette
10:00 - 10:20		**Coffee Break (Main Building)**
10:20 - 12:00	Auditorium Marthe Condat	**Track 1 : Privacy -** Session Chair : Ken Barker **The DCR Delusion: Measuring the Privacy Risk of Synthetic Data.** *Zexi Yao, Natasa Krco, Georgi Ganev and Yves-Alexandre de Montjoye.* **RIPOST: Two-Phase Private Decomposition for Multidimensional Data.** *Ala Eddine Laouir and Abdessamad Imine.* **PriSM: A Privacy-friendly Support vector Machine.** *Michele Barbato, Alberto Ceselli, Sabrina De Capitani di Vimercati, Sara Foresti and Pierangela Samarati.* **Transparency and Consent Challenges in mHealth Apps: An Interdisciplinary Study of Privacy Policies, Data Sharing, and Dark Patterns.** *Mehrdad Bahrini, Alexander Herbst, Merle Freye, Matthias Kohn, Karsten-Sohr and Rainer Malaka*
	Amphitheatre Schwartz	**Track 2 : Attack Analysis 1 -** Session Chair : Edgar Weippl **Zero-Click SnailLoad: From Minimal to No User Interaction.** *Stefan Gast, Nora Puntigam, Simone Franza, Sudheendra Raghav Neela, Daniel Gruss and Johanna Ullrich.* **AcouListener: An Inaudible Acoustic Side-channel Attack on AR/VR.** *Fengliang He, Hong-Ning Dai, Hanyang Guo, Xiapu Luo and Jiadi Yu.* **DBBA: Diffusion-based Backdoor Attacks on Open-set Face Recognition Models.** *Fuqi Qi, Haichang Gao, Boling Li, Guangyu He, Jiacheng Luo and Yuhong Zhang.* **Personalized Password Guessing via Modeling Multiple Leaked Credentials of the Same User.** *Fugeng Huang, Jiahong Yang, Haibo Cheng, Wenting Li and Ping Wang.*
	Auditorium J. Herbrand	**Track 3 : Crypto 1 -** Session Chair : Ximing Fu **Extending Groth16 for Disjunctive Statements.** *Xudong Zhu, Xinxuan Zhang, Xuyang Song, Yi Deng, Yuanju Wei and Liuyu Yang.* **A Certified-Input Mixnet from Two-Party Mercurial Signatures on Randomizable Ciphertexts.** *Masayuki Abe, Masaya Nanri, Miyako Ohkubo, Octavio Perez Kempner, Daniel Slamanig and Mehdi Tibouchi.* **Code Encryption with Intel TME-MK for Control-Flow Enforcement.** *Martin Unterguggenberger, Lukas Lamster, Mathias Oberhuber, Simon Scherer and Stefan Mangard.* **Efficient Homomorphic Evaluation for Non-Polynomial Functions.** *Changhong Xu and Honggang Hu.*

12:00-13:30 **Lunch (Main Building)**

13:30-15:10

Track 4 : Privacy 2 - Session Chair : Emiliia Geloczi

Auditorium Marthe Condat

Membership Privacy Evaluation in Deep Spiking Neural Networks. *Jiaxin Li, Gorka Abad, Stjepan Picek and Mauro Conti.*

Optimized Privacy-Preserving Multi-Signatures from Discrete Logarithm Assumption. *Xiaoyang Wei, Shuai Han and Shengli Liu.*

Functional Credentials: a Practical Construction for the European Digital Identity. *Giovanni Bartolomeo.*

Dobby: A Privacy-Preserving Time Series Data Analytics System with Enforcement of Flexible Policies. *Yansen Xin, Rui Zhang, Zhenglin Fan and Ze Jia*

Track 5 : Detection 1 - Session Chair : Hyungon Moon

Amphitheatre Schwartz

Countering Jailbreak Attacks with Two-Axis Pre-Detection and Conditional Warning Wrappers. *Hyunsik Na, Hajun Kim, Dooshik Yoon and Daeseon Choi.*

WaitWatcher & WaitGuard: Detecting Flush-Based Cache Side-Channels through Spurious Wakeups. *Lukas Lamster, Fabian Rauscher, Martin Unterguggenberger and Stefan Mangard.*

PROTEAN: Federated Intrusion Detection in Non-IID Environments through Prototype-Based Knowledge Sharing. *Sara Chennoufi, Yufei Han, Gregory Blanc, Emiliano De Cristofaro and Christophe Kiennert.*

Machine Learning Vulnerabilities in 6G: Adversarial Attacks and Their Impact on Channel Gain Prediction and Resource Allocation in UC-CF-mMIMO. *Mahmoud Ghorbel, Selina Cheggour, Valeria Loscri, Youcef Imine, Hamza Ouarnoughi and Smail Niar.*

Track 6 : Crypto 2 - Session Chair : Hyeonbum Lee

Auditorium J. Herbrand

Formalisation of KZG commitment schemes in EasyCrypt. *Palak Palak and Thomas Haines.*

Reaction Attack on TFHE: Minimum Number of Oracle Queries and Nearly Optimum Attacking Scheme. *Remma Kumazaki and Yuichi Kaji.*

SafePath: Encryption-less On-demand Input Path Protection For Mobile Devices. *Xin Zhang and Yifan Zhang.*

Polylogarithmic Polynomial Commitment Scheme over Galois Rings. *Zhuo Wu, Xinxuan Zhang, Yi Deng, Yuanju Wei, Zhongliang Zhang and Liuyu Yang.*

15:10-15:40 **Coffee Break (Main Building)**

15:40 - 17:20

Auditorium Marthe Condat

Track 7 : Attack Analysis 2 - Session Chair : Cédrick Austa

LUMIA: Linear probing for Unimodal and MultiModal Membership Inference Attacks leveraging internal LLM states. *Luis Ibanez-Lissen, Lorena González-Manzano, Jose Maria de Fuentes, Nicolas Anciaux and Joaquin Garcia-Alfaro.*

Cache Demote for Fast Eviction Set Construction and Page Table Attribute Leakage. *Taehun Kim, Hyerean Jang and Youngjoo Shin. Epistemology of Rowhammer Attacks: Threats to Rowhammer Research Validity. Martin Heckel, Hannes Weissteiner, Florian Adamsky and Daniel Gruss.*

T-Time: A Fine-grained Timing-based Controlled-Channel Attack against Intel TDX. *Woomin Lee, Taehun Kim, Seunghee Shin, Junbeom Hur and Youngjoo Shin*

Amphitheatre Schwartz

Track 8 : Privacy 3 - Session Chair : Octavio Perez Kempner

Fine-Grained Data Poisoning Attack to Local Differential Privacy Protocols for Key-Value Data. *Terumi Yaguchi and Hiroaki Kikuchi.*

A User-Centric, Privacy-Preserving, and Verifiable Ecosystem for Personal Data Management and Utilization. *Osama Zafar, Mina Namazi, Yuqiao Xu, Youngjin Yoo and Erman Ayday.*

Don't Hash Me Like That: Exposing and Mitigating Hash-Induced Unfairness in Local Differential Privacy. *Berkay Kemal Balioglu, Alireza Khodaie and M. Emre Gursoy.*

Privacy-Preserving Trajectory Data Publication Via Differentially-Private Representation Learning. *Youcef Korichi, Nadia Tawbi, Josee Desharnais and Sebastien Gambs.*

Auditorium J. Herbrand

Track 9 : Crypto 3 - Session Chair : Yohei Watanabe

UTRA: Universal Token Reusability Attack and Token Unforgeable Delegatable Order-Revealing Encryption. *Jaehwan Park, Hyeonbum Lee, Junbeom Hur, Jae Hong Seo and Doowon Kim.*

Efficient Robust Dynamic Searchable Symmetric Encryption Supporting Conjunctive Queries. *Bingxue Bian, Jianfeng Wang and Qiaoer Xu.*

Athena: Accelerating KeySwitch and Bootstrapping for Fully Homomorphic Encryption on CUDA GPU. *Yifan Yang, Kexin Zhang, Peng Xu, Zhaojun Lu, Wei Wang, Weiqi Wang and Kaitai Liang.*

Predicate-Private Asymmetric Searchable Encryption for Conjunctions from Lattices. *Qinyi Li and Xavier Boyen.*

17:20-17:30

Conference Information - Auditorium Marthe Condat

18:30

Welcome Reception at the City-Hall of Toulouse.

Please note that a security check will be carried out at the entrance to the city hall. Unauthorized items will be thrown away (sharp objects, flammable pro-ducts, water bottles, etc.).

Tuesday, September 23, 2025

8:30 - 9:00 — Registration / Welcome Coffee - Main Building

9:00 - 10:00 — Auditorium Marthe Condat

Keynote 2 : «Covert Social Influence Operations: Past, Present, and Future» V.S. Subrahmanian (Northwestern University) - Session Chair : Jaideep Vaidya

10:00 - 10:30 — **Coffee Break (Main Building)**

10:30 - 12:10 — Auditorium Marthe Condat

Track 10 : Blockchain Secured Systems - Session Chair : Hai Dong

Efficient and Secure Sleepy Model for BFT Consensus. *Pengkun Ren, Hai Dong, Zahir Tari and Pengcheng Zhang.*

Premining in the Shadows: How Hidden Blocks Weaken the Security of Proof-of-Work Chains. *Wanying Zeng, Lijia Xie and Xiao Zhang.*

The Economics of Deception: Structural Patterns of Rug Pull across DeFi Blockchains. *Bhavani Kalal, Abdulrahman Alhaidari, Balaji Palanisamy and Shamik Sural.*

Anamorphic Monero Transactions: the Threat of Bypassing Anti-Money Laundering Laws. *Adrian Cinal, Przemysław Kubiak, Mirosław Kutyłowski and Gabriel Wechta.*

Amphitheatre Schwartz

Track 11 : Vulnerability Assessment - Session Chair : Hugo Kermabon

Systematic Assessment of Cache Timing Vulnerabilities on RISC-V Processors. *Cédrick Austa, Jan Tobias Mühlberg and Jean-Michel Dricot.*

A Symbolic Analysis of Hash Functions Vulnerabilities in Maude-NPA. *Arturo Hernández Sánchez and Santiago Escobar.*

FuncVul: An Effective Function Level Vulnerability Detection Model using LLM and Code Chunk. *Sajal Halder, Muhammad Ejaz Ahmed and Seyit Camtepe.*

WelkIR: Flow-Sensitive Pre-trained Embeddings from Compiler IR for Vulnerability Detection. *Hao Huang, Xiuwei Shang, Junqi Zhang, Shaoyin Cheng, Weiming Zhang and Nenghai Yu.*

Auditorium J. Herbrand

Track 12 : Crypto 4 - Session Chair : Kaitai Liang

Tetris! Traceable Extendable Threshold Ring Signatures and More. *Gennaro Avitabile, Vincenzo Botta and Dario Fiore.*

TERRA: Trojan-Resilient Reverse-Firewall for Cryptographic Applications. *Chandan Kumar, Nimish Mishra, Suvradip Chakraborty, Satrajit Ghosh and Debdeep Mukhopadhyay.*

DEBridge: Towards Secure and Practical Plausibly Deniable Encryption Based on USB Bridge Controller. *Chongyu Long, Yuewu Wang, Lingguang Lei, Haoyang Xing and Jiwu Jing.*

Enhanced Key Mismatch Attacks on Lattice-Based KEMs: Multi-bit Inference and Ciphertext Generalization. *Yan Shao, Yuejun Liu, Yongbin Zhou and Mingyao Shao.*

12:10 - 14:00 — **Lunch (Main Building)**

14:00 - 15:40

Auditorium Marthe Condat

Track 13 : AI Security 1 - Session Chair : Gorka Abad

Towards Preventing Free-riders in AI as a Service. *Nuttapong Attrapadung, Goichiro Hanaoka, Ryo Hiromasa, Yoshihiro Koseki, Takahiro Matsuda, Yutaro Nishida, Yusuke Sakai, Jacob Schuldt and Satoshi Yasuda.*

Evaluation of Autonomous Intrusion Response Agents In Adversarial and Normal Scenarios. *Matthew Reaney, Kieran Mclaughlin and Sandra Scott-Hayward*

Let the Noise Speak: Harnessing Noise for a Unified Defense Against Adversarial and Backdoor Attacks. *Md Hasan Shahriar, Ning Wang, Naren Ramakrishnan, Y. Thomas Hou and Wenjing Lou.*

StructTransform: A Scalable Attack Surface for Safety-Aligned Large Language Models. *Shehel Yoosuf, Temoor Ali, Ahmed Lekssays, Mashael Al-Sabah and Issa Khalil.*

Amphitheatre Schwartz

Track 14 : Detection 2 - Session Chair : Nanda Rani

Towards Context-Aware Log Anomaly Detection Using Fine-Tuned Large Language Models. *Hugo Breniaux and Djedjiga Mouheb.*

TATA: Benchmark NIDS Test Sets Assessment and Targeted Augmentation. *Omar Anser, Jérôme François, Isabelle Chrisment and Daishi Kondo.*

GANSec: Enhancing Supervised Wireless Anomaly Detection Robustness through Tailored Conditional GAN Augmentation. *Jiali Xu, Shuo Wang, Valéria Loscrì, Alessandro Brighente, Mauro Conti and Romain Rouvoy.*

GET-AID: Graph-Enhanced Transformer for Provenance-based Advanced Persistent Threats Investigation and Detection. *Zhicheng Huang, Fengyuan Xu, Jiahong Yang, Zonghu Zhang, Wenting Li, Chenbin Zhang, Meng Ma and Ping Wang.*

Auditorium J. Herbrand

Track 15 : Mitigation - Session Chair : Jan Tobias Mühlberg

CapMan: Detecting and Mitigating Linux Capability Abuses at Runtime to Secure Privileged Containers. *Alireza Moghaddas Borhan, Hugo Kermabon-Bobinnec, Lingyu Wang, Yosr Jarraya and Suryadipta Majumdar.*

Verifying DRAM Addressing in Software. *Martin Heckel, Florian Adamsky, Jonas Juffinger, Fabian Rauscher and Daniel Gruss.*

PUSH for Security: A PUF-Based Protocol to Prevent Session Hijacking. *Emiliia Geloczi, Stefan Katzenbeisser and Nico Mexis.*

No Root, No Problem: Automating Linux Least Privilege and Securing Ansible Deployments. *Eddie Billoir, Romain Laborde, Daniele Canavese, Yves Rutschle, Ahmad Samer Wazan and Abdelmalek Benzekri.*

15:40 - 16:10

Coffee Break (Main Building)

16:10-17:50

Auditorium Marthe Condat

Track 16 : AI security 2 - Session Chair : Luis Lissen

SecureT2I: No More Unauthorized Manipulation on AI Generated Images from Prompts. *Xiaodong Wu, Xiangman Li, Qi Li, Jianbing Ni and Rongxing Lu.*

On the Adversarial Robustness of Graph Neural Networks with Graph Reduction. *Kerui Wu, Ka-Ho Chow, Wenqi Wei and Lei Yu.*

DUMB and DUMBer: Is Adversarial Training Worth It in the Real World? *Francesco Marchiori, Marco Alecci, Luca Pajola and Mauro Conti.*

Llama-based source code vulnerability detection: Prompt engineering vs Finetuning. *Dyna Soumhane Ouchebara and Stéphane Dupont.*

Amphitheatre Schwartz

Track 17 : Protection - Session Chair : Junbeom Hur

Formally-verified Security against Forgery of Remote Attestation using SSProve. *Sara Zain, Jannik Mähn, Stefan Köpsell and Sebastian Ertel.*

Trigger-Based Fragile Model Watermarking for Image Transformation Networks. *Preston Robinette, Thuy Dung Nguyen, Samuel Sasaki and Taylor T Johnson.*

Hardening HSM Clusters: Resolving Key Sync Vulnerabilities for Robust CU Isolation. *Sarat Chandra Prasad Gingupalli.*

KeTS: Kernel-based Trust Segmentation against Model Poisoning Attacks. *Ankit Gangwal, Mauro Conti and Tommaso Pauselli.*

Auditorium J. Herbrand

Track 18 : Attack Analysis 3 - Session Chair : Florian Adamsky

Email Cloaking: Deceiving Users and Spam Email Detectors with Invisible HTML Settings. *Bingyang Guo, Mingxuan Liu, Yihui Ma, Ruixun Li, Fan Shi, Min Zhang, Baojun Liu, Chengxi Xu, Haixin Duan, Geng Hong, Min Yang and Qingfeng Pan.*

Correcting the Record on Leakage Abuse Attacks: Revisiting the Subgraph Attacks with Sound Evaluation. *Takumi Namiki, Takumi Amada, Mitsugu Iwamoto and Yohei Watanabe.*

NICraft: Malicious NIC Firmware-based Cache Side-channel Attack. *Amit Pravin Choudhari, Shorya Kumar and Christian Rossow.*

Analysis of input-output mappings in coinjoin transactions with arbitrary values. *Jiri Gavenda, Petr Svenda, Stanislav Bobon and Vladimir Sedlacek.*

17:50 - 18:00

Conference Information - Auditorium Marthe Condat

19:30

Gala Dinner at Hotel Dieu

Wednesday, September 24, 2025

8:30 - 9:00 — Registration / Welcome Coffee - Main Building

9:00 - 10:00 — Auditorium Marthe Condat

Keynote : «Data Privacy and Security in Distributed Collaborative Scenarios» Pierangela Samarati (Universita degli Studi di Milano)
Session Chair : Nora Boulahia-Cuppens

10:00 - 10:30 — **Coffee Break (Main Building)**

10:30 - 12:10

Track 19 : Security Protocols 1 - Session Chair : Sara Zain

Auditorium Marthe Condat

Formal Security Analysis of DNSSEC+. *Ali Sadeghi Jahromi, Abdelrahman Abdou and Paul van Oorschot.*

Hyperion: Transparent End-to-End Verifiable Voting with Coercion Mitigation. *Aditya Damodaran, Simon Rastikian, Peter Roenne and P. Y. A. Ryan.*

Breaking verifiability and vote privacy in CHVote. *Veronique Cortier, Alexandre Debant and Pierrick Gaudry.*

Imitater: An Efficient Shared Mempool Protocol with Application to Byzantine Fault Tolerance. *Qingming Zeng, Mo Li, Ximing Fu, Hui Jiang and Chuanyi Liu.*

Track 20 : Access and Information Flow Control - Session Chair : Emiliia Geloczi

Amphitheatre Schwartz

BlowPrint: Blow-Based Multi-Factor Biometrics for Smartphone User Authentication. *Howard Halim, Eyasu Getahun Chekole, Daniel Reijsbergen and Jianying Zhou.*

An Efficient Security-enhanced Accountable Access Control for Named Data Networking. *Jianfei Sun, Yuxian Li, Xuehuan Yang, Guomin Yang and Robert Deng*

An Algebraic Approach to Asymmetric Delegation and Polymorphic Label Inference. *Silei Ren, Cosku Acay and Andrew C. Myers.*

Identifying Potential Timing Leakages from Hardware Design with Precondition Synthesis. *Minu Chung and Hyungon Moon*

Track 21 : Security Protocols 2 - Session Chair : Fabio De Gaspari

Auditorium J. Herbrand

Unraveling DoH Traces: Padding-Resilient Website Fingerprinting via HTTP/2 Key Frame Sequences. *Baiyang Li, Zhu Yujia, Yuedong Zhang, Qingyun Liu and Li Guo.*

Concretely Efficient Parallel-accessible DORAM for 100K-sized Array. *Koki Hamada*

Efficient One-Pass Private Set Intersection from Pairings with Offline Preprocessing. *Joonsang Baek, Seongbong Choi, Willy Susilo, Partha Sarathi Roy and Hyung Tae Lee.*

VeriFLo: Verifiable Provenance with Fault Localization for Inter-domain Routing. *Utku Tefek, Ertem Esiner, Felix Kottmann and Deming Chen.*

12:10 - 14:00 — **Lunch (Main Building)**

14:00-15:15

Track 22 : Software Testing 2 - Session Chair : Joaquin Garcia-Alfaro

Auditorium Marthe Condat

QUIC-Fuzz: An Effective Greybox Fuzzer For The QUIC Protocol. *Kian Kai Ang and Damith C. Ranasinghe.*

LibAFL*: Fast and State-aware Protocol Fuzzing. *Cristian Daniele, Timme Bethe, Marcello Maugeri, Andrea Continella and Erik Poll.*

Edge Coverage Feedback of Embedded Systems Fuzzing Based on Debugging Interfaces. *Weihua Jiao, Qingbao Li, Xilong Li, Zhifeng Chen, Weiping Yao, Guimin Zhang and Fei Cao.*

Track 23 : Software Testing 1 - Session Chair : Xiao Xi

Amphitheatre Schwartz

NLSaber : Enhancing Netlink Family Fuzzing via Automated Syscall Description Generation. *Lin Ma, Xingwei Lin, Ziming Zhang and Yajin Zhou.*

The Polymorphism Maze: Understanding Diversities and Similarities in Malware Families. *Antonino Vitale, Simone Aonzo, Savino Dambra, Nanda Rani, Lorenzo Ippolito, Platon Kotzias, Juan Caballero and Davide Balzarotti.*

High-Efficiency Fuzzing Technique Using Hooked I/O System Calls for Targeted Input Analysis. *Wenju Sun, Xi Xiao, Qiben Yan, Guangwu Hu, Chuan Chen and Qing Li.*

Track 24 : Attack Analysis 4 - Session Chair : Gregory Blanc

Digital Twin for Adaptive Adversary Emulation in IIoT Control Networks. *Javier Parada, Cristina Alcaraz, Javier Lopez, Juan Caubet and Rodrigo Roman.*

Auditorium J. Herbrand

Efficient End-to-End Non-Profiled Side-Channel Analysis on Long Raw Traces. *Jintong Yu, Yuxuan Wang, Shipei Qu, Yubo Zhao, Yipeng Shi, Pei Cao, Xiangjun Lu, Chi Zhang, Dawu Gu and Cheng Hong.*

The Hidden Dangers of Public Serverless Repositories: An Empirical Security Assessment. *Eduard Marin, Jinwoo Kim, Alessio Pavoni, Mauro Conti and Roberto Di Pietro.*

15:15-15:45

Coffee Break

15:45-17:00

Track 25 : Post-Quantum - Session Chair : Eyasu Getahun Chekole

Auditorium Marthe Condat

A post-quantum Distributed OPRF from the Legendre PRF. *Novak Kaluderovic, Nan Cheng and Katerina Mitrokotsa.*

Security Analysis of Covercrypt: A Quantum-Safe Hybrid Key Encapsulation Mechanism for Hidden Access Policies. *Théophile Brézot, Chloé Hébant, Paola de Perthuis and David Pointcheval*

Two-Factor Authenticated Key Exchange with Enhanced Security from Post-Quantum Assumptions. *Qijia Fan, Chenhao Bao, Xuanyu Shi, Shuai Han and Shengli Liu.*

Track 26 : AI Security 3 - Session Chair : Philippe Owzarski

Amphitheatre Schwartz

Time-Distributed Backdoor Attacks on Federated Spiking Learning. *Gorka Abad, Stjepan Picek and Aitor Urbieta.*

How Dataset Diversity Affects Generalization in ML-based NIDS. *Benoit Nougnanke, Gregory Blanc and Thomas Robert.*

Track 27 : Privacy 4 - Session Chair : Hiroaki Kikuchi

Auditorium J. Herbrand

Privacy-Preserving k-Nearest Neighbor Query: Faster and More Secure. *Jialin Chi, Cheng Hong, Axin Wu, Tianqi Sun, Zhechen Li, Min Zhang and Dengguo Feng.*

Fine-grained, privacy-augmenting LI-compliance in the LAKE standard. *Pascal Lafourcade, Elsa López Pérez, Charles Olivier-Anclin, Cristina Onete, Clément Papon and Mališa Vucinic.*

17:00-17:20 Conference Closing Remarks (awards, announcements and workshops information) - Auditorium Marthe Condat

Conference Keynotes

Keynote 1 - Monday September 23

Out of sight, out of mind: the plumbing problem in Cybersecurity

Carlos Aguilar (SandBoxAQ)

Abstract

Cryptography is the unseen foundation of modern digital security—an essential plumbing system that quietly supports everything from authentication to data protection. Yet, like real plumbing, it is often neglected, hidden away until something breaks. This presentation explores the persistent challenge of cryptographic management: how outdated algorithms, forgotten keys, and ad hoc practices silently undermine cybersecurity. By examining why cryptography so often slips "out of sight, out of mind," we highlight the organizational risks of treating it as an afterthought. Finally, we discuss practical steps—such as systematic cryptographic inventories, lifecycle management, and proactive governance—that can bring visibility and resilience to this critical, but too often overlooked, component of cybersecurity.

Short Bio

Carlos Aguilar Melchor is the Chief Scientist in Cybersecurity at SandboxAQ. In the past he worked as professor for 15 years and as consultant for multiple private sector actors and international organizations, contributing to a variety of domains such as cryptography, privacy, cyber security, and artificial intelligence. He is co-inventor of one of the NIST PQC candidates selected for standardisation, and the author of more than hundred publications.

Keynote 2 - Tuesday September 23

Covert Social Influence Operations: Past, Present, and Future

V.S. Subrahmanian (Northwestern University, USA)

Abstract

Covert Social Influence Operations (CSIOs) have been studied for almost a dozen years. Since a first study of CSIOs in the 2014 Indian election and the DARPA Twitter Influence Bot Detection Challenge of 2015 under the SMISC Program, the field has come a long way. After a quick review of CSIOs of the past, this talk will quickly move on to how recent advances in AI will influence the direction of CSIOs. We can think of CSIOs as involving a threat actor (CSIO operator) targeting a defender (e.g. social platform). Though the extraordinary ability of modern AI to generate realistic text, image, video, audio, and multimodal content poses a potential threat, I will argue that the even more extraordinary ability of AI to dynamically adapt to changing circumstances and defender tactics will likely pose an even bigger threat. (The second part of this talk reflects joint work with Valerio LaGatta and Youzhi Zhang.)

Short Bio

V.S. Subrahmanian is the Walter P. Murphy Professor of Computer Science at the McCormick School of Engineering, Northwestern University and Buffett Faculty Fellow at the Northwestern Roberta Buffett Institute for Global Affairs. He is also the head of the Northwestern Security and AI Laboratory (NSAIL). Prior to this, Subrahmanian was The Dartmouth College Distinguished Professor in Cybersecurity, Technology, and Society at Dartmouth College with tenure in the Computer Science Department and Director of the Institute for Security, Technology and Society (ISTS). Prior to joining Dartmouth, he was a tenured Professor in the University of Maryland's Computer Science Department. He served a 6.5 year stint as Director of the University of Maryland's Institute for Advanced Computer Studies where he co-founded the Lab for Computational Cultural Dynamics and founded the Center for Digital International Government. His work stands squarely at the intersection of data-driven AI for increased security, policy, and business needs. Prof. Subrahmanian has been an invited speaker at the United Nations, Capitol Hill, the Mumbai Stock Exchange, and numerous other prestigious forums.

Keynote 3 - Wednesday September 23

Data Privacy and Security in Distributed Collaborative Scenarios

Pierangela Samarati (Universita degli Studi di Milano, Italia)

Abstract

The availability of highly performing systems and services (e.g., cloud/fog/edge/IoT) for gathering, storing, and processing data, and of analysis techniques on large data collections, bring great benefits on a personal, business, economic and social level. The collection, sharing, and analysis of data, with contributions from different sources and different actors are in fact great enabling factors for the increasingly digitally evolved society. This typically also involves data storage and computation by external providers that may be either not authorized to access information or not fully trusted. In this talk, I will address in particular: the protection of data in collaborative distributed computations involving multiple authorities and providers, the assessment of integrity of outsourced queries and computations, and some privacy challenges and directions in AI/ML scenarios.

Short Bio

Pierangela Samarati is a Professor at the Department of Computer Science of the Università degli Studi di Milano, Italy. Her main research interests are on data and applications security and privacy, especially in emerging scenarios. She has participated in several EU-funded projects involving different aspects of information protection, also serving as project coordinator. She has published more than 300 peer-reviewed articles in international journals, conference proceedings, and book chapters. She has been Computer Scientist in the Computer Science Laboratory at SRI, CA (USA). She has been a visiting researcher at the Computer Science Department of Stanford University, CA (USA), and at the Center for Secure Information Systems of George Mason University, VA (USA). She is the chair of the IEEE Systems Council Technical Committee on Security and Privacy in Complex Information Systems (TCSPCIS), of the ERCIM Security and Trust Management Working Group (STM), and of the ACM Workshop on Privacy in the Electronic Society (WPES). She is a member of several steering committees. She is IEEE Fellow (2012), ACM Fellow (2021), IFIP Fellow (2021). She has received the ESORICS Outstanding Research Award (2018), the IEEE Computer Society Technical Achievement Award (2016), and the IFIP WG 11.3 Outstanding Research Award (2012), and the IFIP TC11 Kristian Beckman Award (2008).

Workshop Program

AutonomousCyber (Amphi Concorde, U4)

Thursday, September 25, 2025

09:00 – 10:30 **Session 1**

Welcome and Opening Remarks

ACSE-Eval: Can LLMs threat model real-world cloud infrastructure? *Sarthak Munshi, Swapnil Pathak, Sonam Ghatode, Thenuga Priyadarshini, Dhivya Chandramouleeswaran and Ashutosh Rana*

Adversarial Evasion against Autonomous Cyber Defence Agents. *Melanie Meijer, Sanyam Vyas, Vasilios Mavroudis and Marc Juarez*

Knowledge Retention for Generic Reinforcement Learning Policies in Autonomous Cyber Defence. *Joshua Sylvester and Rogério de Lemos*

Automated Cyber Defence with Reinforcement Learning in Multi-Attack Environments. *Joshua Sylvester and Rogério de Lemos*

10:30 – 10:50 **Coffee Break (Main Building)**

10:50 - 12:20 **Session 2**

An Explainable Multimodal Framework for Phishing Attack Detection. *Shokooh Khandan, Mohammadreza Tabatabaei, Ifeanyi Bryan Uzoatu, Olamide Jogunola, Yakubu Tsado and Tooska Dargahi*

Risk-Aware SOC Alert Handling in Adaptive Cyber Defense with Reinforcement Learning.*Sajad Homayoun*

Leveraging Large Language Models in Post-Exploitation: Navigating the Cyber Kill Chain with AI-Driven Tactics. *Dean Benson and Christo Panchev*

19:00 **Workshops Dinner**

CBT (Meeting room - Bât. U3)

Thursday, September 25, 2025

09h15-10h30 Welcome and opening remarks (Amphi Condat, Main Building)

Bart preneel - joint keynote with DPM workshop (Amphi Condat, main building)

10h30-10h50 **Coffee Break (Main Building)**

10h50-12h20 **Session 1**

Fast Off-Chain Payments with Second-Layer Privacy. *Sven Gnap, Kari Kostiainen and Ghassan Karame*

AUPCH: Auditable Unlinkable Payment Channel Hubs. *Mohsen Minaei, Pedro Moreno-Sanchez, Srinivasan Raghuraman, Panagiotis Chatzigiannis and Duc Le*

Threshold Signatures for Central Bank Digital Currencies. *Mostafa Abdelrahman, Filip Rezabek, Lars Hupel, Kilian Glas and Georg Carle*

12h20-13h50 **Lunch Break (Main Building)**

13h50-15h20 **Session 2**

Blockchain-Based Lotteries via Single Secret Leader Election. *Tegrid Fettuh and Oguz Yayla*
Towards a Resource Based Blockchain E-Voting System. *Ricardo Almeida, Laura Ricci, Fabrizio Baiardi, Damiano Maesa, Catalin Dragan and Nishanth Sastry*

Analysing the Adoption of Terms of Use in SSI Digital Wallets. *Stefano Bistarelli, Chiara Luchini and Francesco Santini*

15h20-15h40 **Coffee Break (Main Building)**

15h40-17h10 **Session 3**

Multiple Selfish Miners on Nakamoto's Consensus Fruitchain, and Strongchain - An Empirical Evaluation. *Martin Perešíni, Tomáš Hladký, Jakub Kubík and Ivan Homoliak*

EVMpress: Precise Type Inference for Next-Generation EVM Decompilation. *Jung Hyun Kim, Soomin Kim, Jaeseung Choi and Sang Kil Cha*

19:00 **Workshops Dinner**

CPS4CIP (Amphi Schwartz, IMT)

Thursday, September 25, 2025

09:00 – 10:30 **Session 1**

Welcome and Opening Remarks

A Comparative Study of ICS Honeypot Deployments. *Frederik Ondrikov, Denis Donadel, Francesco Lupia, Massimo Merro, Daniel Ricardo dos Santos, Emmanuele Zambon and Nicola Zannone*

Learning-in-the-Middle: Explicit-Recursion Anomaly Detection for Critical Infrastructures. *Peyman Teymoori and Toktam Ramezanifarkhani*

Integration of an OT cybersecurity lab into an industrial automation lab. *Alejandro Manuel López Gómez, Farid Bagheri-Gisour Marandyn, Jaime Mohedano, Atanasio Carrasco, Agustín Valencia, José Antonio Rodríguez-Mondejar, Roberto Gesteira-Miñarro, Néstor Rodríguez Pérez, Rafael Palacios, Javier Jarauta and Gregorio López López*

Designing a NIS2-Compliant Registry System: A Design Science Approach to the Classification and Supervision of Essential and Important Entities. Fabian Aude Steen, Vasileios Mavroeidis, Mateusz Zych and Konstantinos Fysarakis

10:30 – 10:50 **Coffee Break (Main Building)**

10:50 - 12:20 **Session 2**

SecureIoT: Robust AI-Driven Cyber Threat Detection for IoT Applications. *Knut Selstad, Sandeep Pirbhulal, Habtamu Abie, Riku Lehkonen and Ismail Ari Ari*

AI-Guided Test Case Prioritization from Network Traffic in Cyber-Physical Systems. *Valeria Valdés Ríos, Fatiha Zaïdi and Ana Rosa Cavalli*

Improving Machine Learning Models for URL Phishing Detection using Synthetic Data. *Francisco Cardoso, Eva Maia and Isabel Praça*

Federated Learning: An approach with Hybrid Homomorphic Encryption. *Pedro Correia, Ivan Costa, Ivone Amorim, Eva Maia and Isabel Praça*

Conclusion & Planning

19:00 **Workshops Dinner**

CyberICPS - (Amphi J. Herbrant - IRIT)

Thursday, September 25, 2025

09:00 – 10:30	Welcome and opening remarks (Amphi Condat, Main Building)
	Bart preneel - joint keynote with DPM workshop (Amphi Condat, main building)
10:30 – 10:50	**Coffee Break (Main Building)**
10:50 - 12:20	**Session 1** - Chair: Sokratis Katsikas
	Salty Seagull: A VSAT Honeynet to Follow the Bread Crumb of Attacks in Ship Networks, *Georgios Michail Makrakis, Jeroen Pijpker, Remco Hassing, Rob Loves and Stephen McCombie*
	Signals and Symptoms: ICS Attack Dataset from Railway Cyber Range, *Anis Yusof, Yuancheng Liu, Niklaus Kang, Choon Meng Seah, Zhenkai Liang and Chang Ee-Chien*
	Designing and Testing a Low-Cost Electromagnetic Spectrum Attack Threat Monitoring System, *Vassilis Andrianopoulos, Panayiotis Kotzaniko-laou and Christos Douligeris*
12h20-13h50	**Lunch Break (Main Building)**
13h50-15h20	**Session 2 -** Chair: Frédéric Cuppens
	Detecting Anomalous Resource Consumption in Edge AI-Based MQTT Brokers,*Phi Tuong Lau and Stefan Katzenbeisser*
	CRLF: A Sim2Real Reinforcement Learning Environment for Automated IT/OT Pentesting, *Marc-Antoine Faillon, Julien Francq, Frédéric Cuppens, Nora Boulahia-Cuppens and Reda Yaich*
	From Words to Wires: Leveraging LLMs for Rapid ICS Cyber-Range Construction, *Tommy Berg, Ahmed Amro, Aida Akbarzadeh and Georgios Kavallieratos*
15h20-15h40	**Coffee break (Main Building)**
15h40-17h10	**Session 3** - Chair: Nora Cuppens-Boulahia
	In Numeris Veritas: An Empirical Measurement of Wi-Fi Integration in Industry.*Vyron Kampourakis, Christos Smiliotopoulos, Vasileios Gkioulos and Sokratis Katsikas*
	Using Dual Algorithm Certificates in TLS: Enabling Rapid Transition to Post-Quantum Cryptography with Backward Compatibility.*Tobias Frauenschläger and Juergen Prof. Dr. Mottok*
	Secure and Efficient Attribute-based Signature Scheme for Substation Automation Systems. Mohammed Ramadan, Moritz Gstür, Pranit Gadekar, Ghada Elbez and Veit Hagenmeyer
19:00	**Workshops Dinner**

DiSA (Room 01, IRIT)

Thursday, September 25, 2025

09:00 – 10:30	**Session 1**
10:50 - 12:20	Short welcome
	Protecting Society from Fake Advertisement Campaigns: Innovative Graph Based Analysis and Approach, *Ewelina Bartuzi-Trokielewicz, Alicja Martinek, Rafał Kozik, Michał Choras*

Adapting Epidemic Contact Models to Misinformation Spread via Social Networks, *Lankeshwara Munasinghe and Christopher Mcdermott*

POLfake: relational dataset for Polish fake news detection, *Mateusz Walczak, Aneta Poniszewska-Maranda*

Transparent and Trustworthy eXpainable AI (xAI) in Smart Human-Robot Collaboration Environment, *Michał Choras, Aleksandra Pawlicka, Marek Pawlicki, Rafal Kozik.*

19:00 **Workshops Dinner**

DPM (Auditorium Marthe Condat - Main Building)

Thursday, September 25, 2025

09:15 – 10:30 Welcome and opening remarks

Bart preneel - joint keynote with DPM workshop

10:30-10:50 **Coffee Break (Main Building)**

10:50-12:25 **Session 1** , session chair Ken Barker (University of Calgary)

How Worrying Are Privacy Attacks Against Machine Learning? *Josep Domingo-Ferrer*

Lost in the Averages: Reassessing Record-Specific Privacy Risk Evaluation. *Yves-Alexandre de Montjoye, Natasa Krco, Matthieu Meeus, Bogdan Kulynych*

Membership Inference Attacks Beyond Overfitting. *Mona Khalil, Alberto Blanco-Justicia, Najeeb Jebreel, Josep Domingo-Ferrer*

«Why is the sky blue?» – On the feasibility of privacy-friendly conversational LLM smart toys. *Isabel Wagner, Valentyna Pavliv, Luigi Lazri, Jan Buechele*

Win-k: Improved Membership Inference Attacks on Small Language Models. *M. Emre Gursoy, Roya Arkhammadova, Hosein Madadi Tamar*

12:25-13:50 **Lunch Break (Main Building)**

13:50 - 15:20 **Session 2** *(Amphi Condat, Main Building), session chair Guillermo Navarro-Arribas (Universitat Autonoma de Barcelona)*

Advanced Electronic Signatures and GDPR: Reconciling the Concepts. *Miroslaw Kutylowski, Paweł Kostkiewicz, Gabriel Wechta*

Invisible Encryption. *Shahzad Ahmad, Stefan Rass, Zahra Seyedi*

Eliminating Exponential Key Growth in PRG-Based Distributed Point Functions. *Marc Damie, Florian Hahn, Andreas Peter, Jan Ramon*

A Pseudo-Inverse Matrix-Based LDP for High-Dimensional Data, *Hiroaki Kikuchi*

Using Prior Knowledge to Improve GANs for Tabular Data Without Compromising Privacy, *Sonakshi Garg, Marcel Neunhoeffer, Jörg Drechsler, Vicenc Torra*

Coffee break (Main Building)

Session 3 *(Amphi Condat, Main Building), session chair Joaquin Garcia-Alfaro (Institut Polytechnique de Paris)*

Lessons from a Robotaxi: Challenges in Selecting Privacy-Enhancing Technologies, *Sebastian Pape, Ala'A Al-Momani, David Balenson, Christoph Bösch, Zoltán Ádám Mann, Jonathan Petit*

Performance Analysis of Lightweight Transformer Models for Healthcare Application Privacy Threat Detection, *Jude Ameh, Abayomi Otebolaku, Alex Shenfield, Augustine Ikpehai, Dauda Sule*

15:20-15:40 **The Bitter Pill: Tracking and Remarketing on EU Pharmacy Websites**, *Zahra Moti, Kimberley Frings, Christine Utz, Frederik Zuiderveen Borgesius, Gunes Acar*

15:40-17:10 **PADOME: Adaptive Privacy Assistant for the Internet of Things,** *Edward Rochester, Ken Barker*

19:00 **Workshops Dinner**

HS3 (Thesis Room, IRIT)

Thursday, September 25, 2025

09:15 – 10:30 **Session 1:** *Attacks & Vulnerabilities*

OpenGL GPU-Based Rowhammer Attack, *Antoine Plin, Frédéric Fauberteau and Nga Nguyen*

Cache Attacks in Modern/Multi-socket x86 Systems (Work in Progress), *Guillaume Didier, Augustin Lucas and Thomas Rokicki*

Revealing Embedded System Behaviors: A Comparative Analysis of Power Consumption and Hardware Performance Counters, *Mohammed Mezaouli, Yehya Nasser, Samir Saoudi and Marc-Oliver Pahl*

Germany Is Rolling Out Nation-Scale Key Escrow And Nobody Is Talking About It, *Jan Sebastian Götte*

10:30-10:50 **Coffee Break (Main Building)**

10:50-12:25 **Session 2:** *Defences & Anomaly Detection*

Hardware Performance Counters for Anomaly Detection in Embedded Devices, *Victor Breux and Pierre-Henri Thevenon*

Semantic-Aware Provenance-Based Intrusion Detection for Edge Systems, *Qingyu Zeng, Songxuan Liu, Yu Wu and Yuko Hara*

Inter-Device PUFs: A Novel Paradigm for Physical Unclonable Functions, *Emiliia Geloczi and Stefan Katzenbeisser*

Mitigation of the impact of Virtual Machine Introspection Pauses on Multi-core Virtual Machines, *Léo Cosseron, Louis Rilling and Martin Quinson*

12:20-13:50 **Lunch Break (Main Building)**

13:50-15:20 *Session 3: Invited Talk*

13:50-15:40 **Coffee Break (Main Building)**

15:40-16:30 *Session 4: Verification and Validation*

heRVé: towards a formally verified RISC-V processor with security mechanisms (Work in Progress), *Cyprien Jules, Pierre Wilke, Guillaume Hiet and Gabriel Desfrene*
InSight - A CoreSight Trace Interpreter for Dynamic Information Flow Tracking (Work in Progress), *Quentin Ducasse, Guillaume Hiet, Volker Stolz and Pierre Wilke*

16:30 *Open Discussion & Closing*

19:00 **Workshops Dinner**

STMUS (Room 01, IRIT)

Thursday, September 25, 2025

11:00-11:15	*Opening Remarks*
11:15-12:15	**Session 1**
	Overview of Machine Unlearning in Fostering Responsible and Adaptive AI in Education Context. *Betty Mayeku, Sandra Hummel and Parisa Memarmoshrefi*
	Adversarial Federated Unlearning with Representation Decoupling.*Yu Jiang, Kwok-Yan Lam and Chee Wei Tan*
12:15-13:50	Lunch Break (Main Building)
14:00-15:00	**Session 2**
	Machine Unlearning of Multilingual Transformers for Kazakh Text Classification. *Milana Bolatbek and Shynar Mussiraliyeva*
15:00 - 15:30	Coffee Break (Main Building)
15:30-16:00	**Session 3**
	When Forgetting Reveals: Black-Box Inversion Attacks on Unlearning in Large Language Models. *Zijun Zhang, Bang Wu and Xingliang Yuan*
16:00-16:50	*Discussion (Participants: TBD)*
16:50-17:00	*Concluding Remarks*
19:00	**Workshops Dinner**

SECAI (Amphi Schwartz, IMT)

Thursday, September 25, 2025

13:50-14:00	Welcome
14:00-15:15	**Session 1**
	On the Effectiveness of Generative Adversarial Networks for data augmentation in malware detection, *Giovanni Ciaramella, Fabio Martinelli, Antonella Santone and Francesco Mercaldo*
	An Adaptive Self-guarded and Risk-Aware Honeypot using DRL, *Sereysethy Touch and Jean-Noël Colin*
	Simplicity Performs, But Should It? Examining Malware Detection Benchmark Datasets, *Samy Bettaieb, Laurens D'hooge, Charles-Henry Bertrand Van Ouytsel, Axel Legay, Etienne Rivière, Miel Verkerken and Bruno Volckaert*
15:15-15:35	Coffee Break (Main Building)
15:35-17:10	**Session 2**
	One Size Doesn't Fit All: A Dynamic Heterogeneous Learning Ensemble for Malware Family Classification, *Solomon Sonya, Muqi Zou, Saastha Vasan, Christopher Kruegel, Giovanni Vigna and Dongyan Xu*
	Evaluating The Explainability of Deep Learning-based Network Intrusion Detection Systems, *Ayush Kumar and Vrizlynn Thing*
	In-context learning for the classification of manipulation techniques in phishing emails, *Antony Dalmiere, Guillaume Auriol, Vincent Nicomette and Pascal Marchand*

Evaluating the Capabilities of AI-based Penetration Testing Tools, *Jacques Ophoff, Ibeabuchi Egbu and Sanaz Kavianpour*

19:00 **Workshops Dinner**

Friday, September 26, 2025

09:00 – 10:35 **Session 3**

Diffusion or Non-Diffusion Adversarial Defenses: Rethinking the Relation between Classifier and Adversarial Purifier, *Yuan-Chih Chen and Chun-Shien Lu*

Scalable Generation of Invariance-Based Adversarial Examples Using XAI, *Samuel Oberhofer, Martin Nocker, Florian Merkle and Pascal Schöttle*

Analysing Safety Risks in LLMs Fine-Tuned with Pseudo-Malicious Cyber Security Data, *Adel Elzemity, Budi Arief and Shujun Li*

Towards a Systematic Risk Assessment of Deep Neural Network Limitations in Autonomous Driving Perception, *Svetlana Pavlitska, Christopher Gerking and J. Marius Zöllner*

10:35 – 10:55 **Coffee Break (IRIT)**

10:55 - 12:10 **Session 4**

Backdoor Attacks on Transformers for Tabular Data: An Empirical Study, *Bart Pleiter, Behrad Tajalli, Stefanos Koffas, Gorka Abad, Jing Xu, Martha Larson and Stjepan Picek*

Strategic Sample Selection for Improved Clean-Label Backdoor Attacks in Text Classification, *Onur Alp Kirci and M. Emre Gursoy*

Towards Automated Threat Elicitation from the AI Act, *Simone Di Mauro, Mario Raciti and Giampaolo Bella*

12:10-13:50 **Lunch Break (Main Building)**

13:50-15:50 **Session 5**

Methodology for Systematic Security Testing of LLM-based Applications, *Dawid Nastaj and Wojciech Mazurczyk*

Adaptive Token-Weighted Differential Privacy for LLMs: Not All Tokens Require Equal Protection, *Manjiang Yu, Priyanka Singh, Xue Li and Yang Cao*

Does Retrieval-Augmented Generation Mitigate Training Data Leakage Risks from Large Language Models?, *Tsunato Nakai, Takuya Higashi and Kento Oonishi*

From Legacy to Standard: LLM-Assisted Transformation of Cybersecurity Playbooks into CACAO Format, *Mehdi Akbari Gurabi, Lasse Nitz, Radu-Mihai Castravet, Roman Matzutt, Avikarsha Mandal and Stefan Decker*

Prompt Infection: LLM-to-LLM Prompt Injection within Multi-Agent Systems, *Donghyun Lee, Mo Tiwari and Brando Miranda*

15:50 - 16:00 Best Paper Award and Closing

STM (Amphi Concorde, U4)

Thursday, September 25, 2025

13:30 - 13:45 Welcome session

13:45 - 14:45 ERCIM STM AWARD 2025 Presentation

14:45 - 15:00 **Coffee Break (Main Building)**

15:00 - 17:00 **Session 1:** Identity Manag., Authentication, Access Control & Formal Modeling

Toward Secure and Trustworthy Identity Management Systems: A Knowledge-base Driven Approach, *Gianluca Sassetti, Amir Sharif, Roberto Carbone and Silvio Ranise*

Always Authenticated, Never Exposed: Continuous Authentication via Zero-Knowledge Proofs, *Dennis Hamm, Erwin Kupris and Thomas Schreck*
Pragmatic guidelines for formal modeling of security ceremonies, Barbara Fila and Ermenda Hoxha

Access Control Administration for Smart Homes, *Clara Bertolissi and Maribel Fernandez*

19:00 **Workshops Dinner**

Friday, September 26, 2025

09:30 – 10:30 Keynote Session

10:50 - 12:20 **Session 2:** AI & Machine Learning For Security (Session Chair: Cristina Alcaraz)

Parameter-Efficient Fine-Tuning of LLMs for Intrusion Detection and Firewall Rule Generation: A Comparative Study, *Chi Zhang, Muhammad Shadi Hajar, Harsha Kalutarage and Lankeshwara Munasinghe*

ABusing social media & sentiment analysis for stock market prediction, *Crawford Brown, Nikolaos Pitropakis, Christos Chrysoulas and Costas Lambrinoudakis*

DrATC+: A Divide et Impera Extension to Trust-Based Dynamic Routing, *Davide Ferraris, Letizia Russo and Lorenzo Monti*

12:20 – 13:50 **Lunch Break (Main Building)**

13:50 - 15:20 **Session 3:** Cybersecurity Strategies, Regulations, Privacy Session

How to Train Your Guardian: Evaluating Cyber Security Exercises Using Situation Awareness *Håvard J. Ofte and Sokratis Katsikas*

Towards an architecture for managing security under the EU Cyber Resilience Act *Daniele Canavese, Afonso Ferreira, Romain Laborde and Mohamed Ali Kandi*

Google Tag Manager and its Privacy Issues *Javiera Alegría Dinamarca, Ivana Bachmann and Javier Bustos-Jiménez*

15:20-15:30 **Coffee Break (IRIT)**

15:30-17:00 **Session 4:** Cryptography & Threat Analysis

Measuring Modern Phishing Tactics: A Quantitative Study of Body Obfuscation Prevalence, Co-occurrence, and Filter Impact, Antony Dalmiere, Zheng Zhou, Guillaume Auriol, Vincent Nicomette and Pascal Marchand

Nicknames for Group Signatures, Guillaume Quispe, Pierre Jouvelot and Gérard Memmi

The Impact of Filtering in Differential Cryptanalysis: A Case Study on FEAL-8, Ivan Costa, Ivone Amorim, Eva Maia and Isabel Praça

17:00 - 17:10 Closing Session

ANUBIS (Amphi J. Herbrant - IRIT)

Friday, September 25, 2025

09:00 - 10:10 **Keynote: Digital Twins for Cyberdefense, Cristina Alcaraz**

No Bot Allowed: Detection of Automated Traffic on Modern Booking Platforms. Methods, Insights, and Current Challenges, *Umberto Fontana, Elisa Chiapponi, Claudio Costanza, Vincent Rigal, Olivier Thonnard, Martynas Buozis and Herve Debar*

10:30-10:50	**Coffee Break (IRIT)**
10:50-12:20	**Session** 1
	HENDRICS: A Hardware-in-the-Loop Testbed for Enhanced Intrusion Detection, Response and Recovery of Industrial Control Systems, *Lalie Arnoud, Zoé Lagache, Pierre-Henri Thevenon, Aloïs Champenois, Victor Breux, Maxime Puys, Eric Gaussier and Oum-El-Kheir Aktouf*
	Get out of DEDALE with RESCOUSSE: a New Dataset and Testbed for Evaluating the Detection of APT attacks among Network and System Logs, *Maxime Lanvin and Frédéric Majorczyk*
	Superviz25-SQL: High-Quality Dataset to Empower Unsupervised SQL Injection Detection Systems, *Grégor Quetel, Eric Alata, Pierre-François Gimenez, Laurent Pautet and Thomas Robert*
12:20 - 13:50	**Lunch Break (Main Building)**
13:50 - 15:20	**Session 2**
	Middlebox Assessment and Network Gaps: Observing Enforced Security *Alya Alshaikh, Ilies Benhabbour and Marc Dacier*
	Network Intrusion Response Systems: Towards standardized evaluation of intrusion response *Thomas Marchioro, Rachida Saroui and Alexis Olivereau*
	Nxcap: A Unified Format for NIDS Benchmarking *Gabin Noblet, Cédric Lefebvre, Philippe Owezarski and William Ritchie*
15:20 - 15:40	**Coffee Break (IRIT)**
15:40 - 17:10	**Session 3**
	Synthetic Network Traffic Generation for Intrusion Detection Systems: a Systematic Literature Review *Pierre-François Gimenez*
	Constraint-based Network Topology Generation for Evaluating Federated Intrusion Detection Systems *Léo Lavaur, Fabien Autrel and Yann Busnel*

SecAssure (Meeting room - Bât. U3)

Friday, September 25, 2025

09:30 – 10:30	**Session 1:** Introduction and Keynote, Chair: Basel Katt
	Welcome and Opening Remarks
	Keynote Speaker
	CybAlliance and ERA 4.0 project presentation
10:30 - 10:50	**Coffee Break (IRIT)**
10:50 - 12:20	**Session 2:** Cloud & Microservices Security Assurance, Chair: Ankur Shukla
	Noisy Neighbor: Exploiting RDMA for Resource Exhaustion Attacks in Containerized Clouds, *Gunwoo Kim, Taejune Park and Jinwoo Kim*
	ConLock: Reducing Runtime Attack Surface in Containerized Microservices, *Asbat El Khairi, Andreas Peter and Andrea Continella*
	Towards Zero-Knowledge Based Private and Verifiable Software Assurance, *Karl Norrman, Björn Johansson and Ferhat Karakoc*
12:20 - 13:50	**Lunch Break (Main Building)**
13:50 - 15:20	**Session 3**: Policy, Compliance & Threat Assurance, Chair: Sandeep Pirbhulal

Assessing the State of Proactive Data Usage Control Enforcement, *Monika Kamhuber, Sascha Wessel and Joana Pecholt*

Modelling Offensive Security Killchains from Compliance Gaps with Security Directives, *Gianpietro Castiglione and Giampaolo Bella*

Security Management of Threats with CyberGraph, *Ettore Carbone, Paolo Falcarin, Purbasha Chowdhury, Francesco Bruno and Fabio Dainese*

15:20 - 15:40 Coffee Break (IRIT)

15:40 - 17:10 **Session 4**: Group Discussion and Closing Remarks

Group Discussion: Security Assurance and Emergency Technologies: Challenges and Innovations

MIST (Thesis Room, IRIT)

Friday, September 25, 2025

9:00-10:30 **Session 1**
Welcome speech + Keynote

Streamlining Security Patches and Remote Attestations for the Internet of Things, *Konrad-Felix Krentz*

10:30-10:50 Coffee Break (IRIT)

10:50-12:20 **Session 2**

Lightweight IoT Intrusion Detection with Hybrid Feature Selection and CNN-Driven Image Transformation, *Negar Mansouri, Seyedeh Leili Mirtaheri, Seyyed Amir Asghari and Andrea Pugliese*

Breaking the Silence: Fuzzing LTE-M and NB-IoT protocols, *Ilja Siroš, Rafael Cavalcanti, Dave Singelée and Bart Preneel*

Function-Level Syscall Fingerprinting for IoT Malware Capability Classification, *Yutaro Osako, Hayato Hamano, Yuto Aono, Toshihiro Yamauchi, Katsunari Yoshioka, Takahiro Kasama, Takuya Fujihashi and Shunsuke Saruwatari*

Permission Granted? How Android's App List Protection Fails in Practice, *Julian Gagel, Kris Heid and Jens Heider*

12:20 - 13:50 Lunch Break (Main Building)

13:50 - 15:20 **Session 3**

Revisiting the Effectiveness of Jailbreak Detection, *Muhammad Irfan and Nelson Uto*

PIM: A Metric to Empower Mobile App Users in Privacy Management, *Amador Aparicio, M. Mercedes Martínez-González, Alejandro Pérez-Fuente and Pablo A. Criado-Lozano*

Policy Enforcement Protocols with Split Keys, *Gizem Akman, Philip Ginzboorg, Sampo Sovio and Valtteri Niemi*

Closing

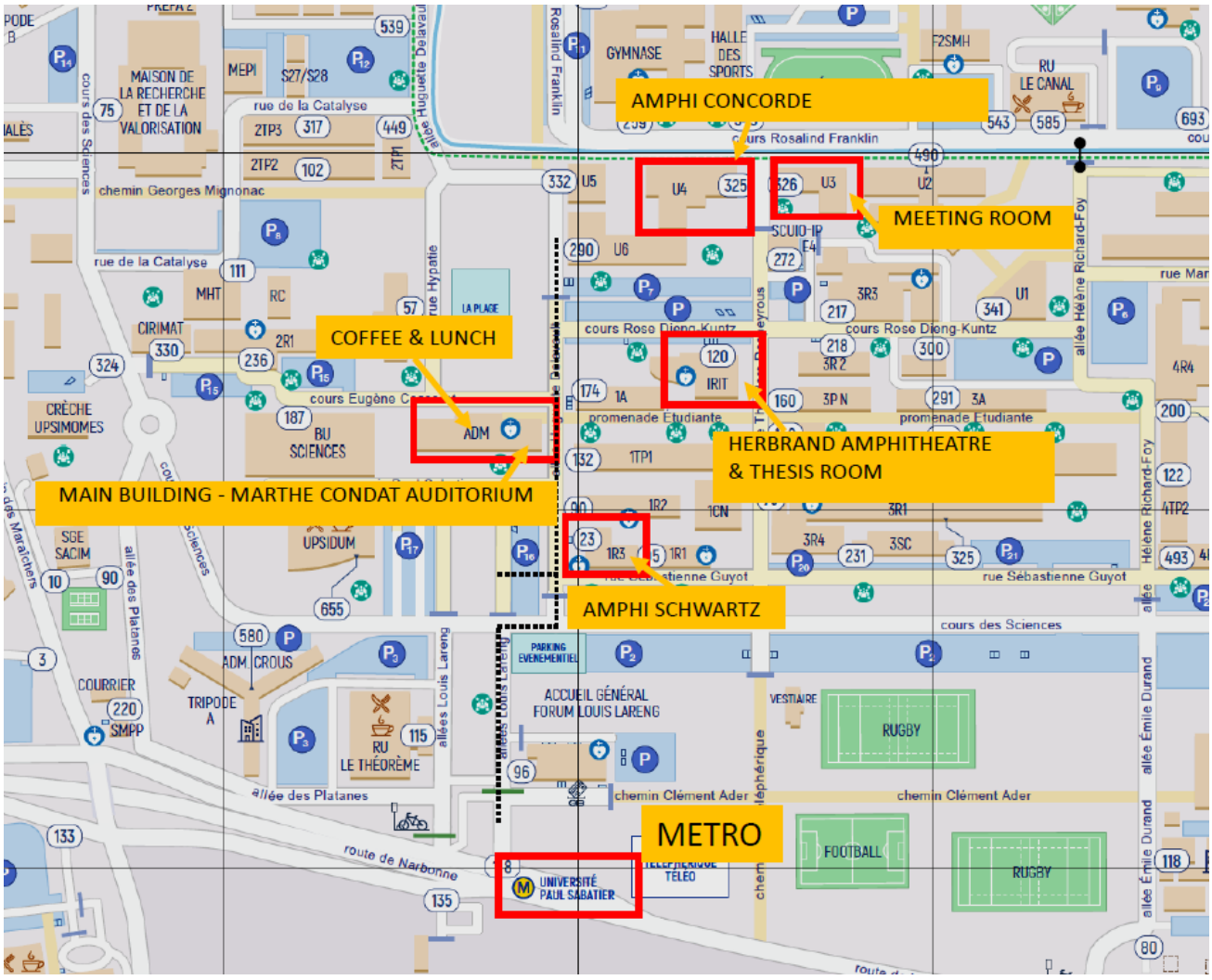
15:20 - 15:40 Coffee Break (IRIT)

Venue

Toulouse University

The Conference and the workshops are taking place in Toulouse University Campus.

Most of the activities will take place in the central building, e.g. congres desk, sessions in the Marthe Condat Auditorium, coffee and lunch breaks. But we have also access to more lecture halls in in the neighboring to organise the various sessions of the program.



Venue

Welcome Reception at the City-Hall of Toulouse

Please note that a security check will be carried out at the entrance to the city hall. Unauthorized items will be thrown away (sharp objects, flammable products, water bottles, etc.).

Kick off the conference with a delightful Welcome Cocktail at the Capitol.

Date: Monday, September 22
Time: 18:30
Venue: City-Hall of Toulouse - The Capitol

Gala Dinner at the Hotel Dieu

The conference dinner will be held in the Hotel Dieu, which is one of the iconic historical buildings of Toulouse. It is situated on the western bank of the Garonne River and offers a splendid view on the city center of Toulouse. The access is very easy and the Hotel Dieu is in walking distance of most hotels in the City Center.

Date: Tuesday, September 23
Time: 19:30
Venue: Hotel Dieu
Address: 2 Rue Charles Viguerie, 31300 Toulouse
Nearest Metro Station: St Cyprien - République

Workshops dinner - Garonne Cruise

The workshops dinner will offer a unique opportunity to continue fruitful discussions while cruising along the Garonne River, accompanied by a refreshing cocktail reception.

Date: Thursday, September 25
Time: 19:00
Venue: Péniches «Les Bâteaux Toulousains»
Address: Port de la Daurade, 31000 TOULOUSE
Nearest Metro Station: Carmes or Esquirol

Sponsors

Contact us

- esorics2025@sciencesconf.org
- https://esorics2025.sciencesconf.org