

2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P 2025)

**Venice, Italy
30 June - 4 July 2025**

Pages 1-584



**IEEE Catalog Number: CFP25C75-POD
ISBN: 979-8-3315-9494-7**

**Copyright © 2025 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP25C75-POD
ISBN (Print-On-Demand):	979-8-3315-9494-7
ISBN (Online):	979-8-3315-9493-0
ISSN:	2995-1348

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2025 10th IEEE European Symposium on Security and Privacy (EuroS&P) **EuroSP 2025**

Table of Contents

Message from the General Chairs	xii
Message from the Program Chairs	xiii
Organizing Committee	xiv
Program Committee	xv
Steering Committee	xviii

Privacy

A Systematic Study of Practical & Formal Privacy in the 5G AKMA Procedure	1
<i>Ioana Boureanu (Surrey Centre for Cyber Security, University of Surrey), Stephan Wesemeyer (Surrey Centre for Cyber Security, University of Surrey), Fortunat Rajaona (Surrey Centre for Cyber Security, University of Surrey), Steve Schneider (Surrey Centre for Cyber Security, University of Surrey), and Helen Treharne (Surrey Centre for Cyber Security, University of Surrey)</i>	
Active Attribute Inference Against Well-Generalized Models In Federated Learning	17
<i>Catarina Gomes (University of Porto, Portugal), Ricardo Mendes (University of Coimbra, Portugal), and João P. Vilela (University of Porto, Portugal)</i>	
Scalable and Fine-Tuned Privacy Pass from Group Verifiable Random Functions	38
<i>Dennis Faut (Karlsruhe Institute of Technology, University of Luxembourg), Andy Rupp (Karlsruhe Institute of Technology, University of Luxembourg), Lisa Kohl (Centrum Wiskunde & Informatica (CWI)), and Julia Hesse (IBM Research Europe)</i>	
TAPShield: Securing Trigger-Action Platforms against Strong Attackers	60
<i>Mojtaba Moazen (KTH Royal Institute of Technology), Nicolae Paladi (CanaryBit AB and Lund University), Adnan Jamil Ahsan (KTH Royal Institute of Technology), and Musard Balliu (KTH Royal Institute of Technology)</i>	
They See Me Scooting — A Long-Term Real-World Data Analysis of Shared Micro-Mobility Services and their Privacy Leakage	78
<i>Karina Elzer (DTU Technical University of Denmark, Denmark), Eric Jedermann (RPTU University of Kaiserslautern, Germany), Stefanie Roos (RPTU University of Kaiserslautern, Germany), and Jens Schmitt (RPTU University of Kaiserslautern, Germany)</i>	
You Can't Trust Your Tag Neither: Privacy Leaks and Potential Legal Violations within the Google Tag Manager	93
<i>Gilles Mertens (Inria), Nataliia Bielova (Inria), Vincent Roca (Inria), and Cristiana Santos (Utrecht University School of Law)</i>	

Your Car Tells Me Where You Drove: A Novel Path Inference Attack via CAN Bus and OBD-II Data	113
<i>Tommaso Bianchi (University of Padova, Italy), Alessandro Brighente (University of Padova, Italy), Mauro Conti (University of Padova, Italy), Delft University of Technology, Netherlands), and Andrea Valori (Innova Trieste S.p.A.,Italy)</i>	

User, Web & Measurement

All that Glitters is not Gold: Uncovering Exposed Industrial Control Systems and Honeypots in the Wild	133
<i>Martin Mladenov (Delft University of Technology, The Netherlands), László Erdődi (Norwegian University of Science and Technology, Norway), and Georgios Smaragdakis (Delft University of Technology, The Netherlands)</i>	
CHARON: Polyglot Code Analysis for Detecting Vulnerabilities in Scripting Languages Native Extensions	153
<i>Raoul Scholtes (CISPA Helmholtz Center for Information Security, Germany), Soheil Khodayari (CISPA Helmholtz Center for Information Security, Germany), Cristian-Alexandru Staicu (CISPA Helmholtz Center for Information Security, Germany), and Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany)</i>	
Demystifying the Perceptions Gap Between Designers and Practitioners in Two Security Standards	169
<i>Shreyas Kumar (Texas A&M University)</i>	
Dredging the River Styx: Fortifying the Web through Robust and Real-Time Script Attribution	188
<i>Kostas Drakonakis (Technical University of Crete, Greece), Sotiris Ioannidis (Technical University of Crete, Greece), and Jason Polakis (University of Illinois Chicago, USA)</i>	
Enhancing Cybersecurity Awareness in Small and Medium Enterprises Through a User-Friendly Risk Assessment Tool	209
<i>Miriam Curtin (Munster Technological University), Brian Sheehan (Munster Technological University), Melanie Gruben (Munster Technological University), Gillian O'Carroll (Munster Technological University), and Hazel Murray (Munster Technological University)</i>	
Exploring the Design Space for Security Warnings in Immersive Environments	227
<i>Andrea Mengascini (CISPA Helmholtz Center for Information Security, Germany), Annabelle Walle (CISPA Helmholtz Center for Information Security, Germany), Rebecca Weil (CISPA Helmholtz Center for Information Security, Germany), Jürgen Steimle (Saarland University, Germany), and Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany)</i>	
Incentivizing Security Excellence in Cyber Liability Insurance	251
<i>Shreyas Kumar (Texas A&M University)</i>	
MalMixer: Few-Shot Malware Classification with Retrieval-Augmented Semi-Supervised Learning	268
<i>Jiliang Li (Stanford University), Yifan Zhang (Vanderbilt University), Yu Huang (Vanderbilt University), and Kevin Leach (Vanderbilt University)</i>	

Port Forwarding Services Are Forwarding Security Risks	289
<i>Haoyuan Wang (University of Science and Technology of China), Yue Xue (University of Science and Technology of China), Xuan Feng (Microsoft Research), Chao Zhou (University of Science and Technology of China), and Xianghang Mi (University of Science and Technology of China)</i>	
WWXSS: Systematic Study, and Large-Scale Measurement of Cross-Site Scripting (XSS) in Web Workers Contexts	304
<i>Dolière Francis Somé (CISPA Helmholtz Center for Information Security)</i>	

Systems

KubeKeeper: Protecting Kubernetes Secrets Against Excessive Permissions	322
<i>Maryam Rostamipoor (Stony Brook University), Aliakbar Sadeghi (Stony Brook University), and Michalis Polychronakis (Stony Brook University)</i>	
LATTE: Layered Attestation for Portable Enclaved Applications	339
<i>Haoxuan Xu (Shanghai Jiao Tong University, China), Jia Xiang (Shanghai Jiao Tong University, China), Zhen Huang (Shanghai Jiao Tong University, China), Guoxing Chen (Shanghai Jiao Tong University, China), Yan Meng (Shanghai Jiao Tong University, China), and Haojin Zhu (Shanghai Jiao Tong University, China)</i>	
LibAFLGo: Evaluating and Advancing Directed Greybox Fuzzing	355
<i>Elia Geretto (Vrije Universiteit Amsterdam, Amsterdam, the Netherlands), Andrea Jemmett (Vrije Universiteit Amsterdam, Amsterdam, the Netherlands), Cristiano Giuffrida (Vrije Universiteit Amsterdam, Amsterdam, the Netherlands), and Herbert Bos (Vrije Universiteit Amsterdam, Amsterdam, the Netherlands)</i>	
PreFence: A Fine-Grained and Scheduling-Aware Defense Against Prefetching-Based Attacks .	374
<i>Till Schlüter (CISPA Helmholtz Center for Information Security) and Nils Ole Tippenhauer (CISPA Helmholtz Center for Information Security)</i>	
Rubicon: Precise Microarchitectural Attacks with Page-Granular Massaging	395
<i>Matej Bölskei (ETH Zurich), Patrick Jattke (ETH Zurich), Johannes Wikner (ETH Zurich), and Kaveh Razavi (ETH Zurich)</i>	
SoK: No Goto, No Cry? The Fairy Tale of Flawless Control-Flow Structuring	411
<i>Eva-Maria C. Behner (Fraunhofer FKIE, Germany), Steffen Enders (Fraunhofer FKIE, Germany), and Elmar Padilla (Fraunhofer FKIE, Germany)</i>	
SoK: Security of EMV Contactless Payment Systems	432
<i>Mahshid Mehr Nezhad (University of Warwick, UK), Feng Hao (University of Warwick, UK), Gregory Epiphaniou (University of Warwick, UK), Carsten Maple (University of Warwick, UK), and Timur Yunusov (Payment Village, UK)</i>	

Crypto

Attacking and Fixing the Android Protected Confirmation Protocol	458
<i>Myrto Arapinis (The University of Edinburgh), Vincent Danos (CNRS, Ecole Normale Supérieure), Maïwenn Racouchot (CISPA Helmholtz Center for Information Security), David A. R. Robin (Ecole Normale Supérieure), and Thomas Zacharias (University of Glasgow)</i>	

Best-Possible Unpredictable Proof-of-Stake: An Impossibility and a Practical Design	480
<i>Lei Fan (Shanghai Jiao Tong University, China), Jonathan Katz (Google, USA), Zhenghao Lu (Shanghai Jiao Tong University, China), Phuc Thai (Sky Mavis, Vietnam), and Hong-Sheng Zhou (Virginia Commonwealth University, USA)</i>	
Commitment Attacks on Ethereum’s Reward Mechanism	504
<i>Roozbeh Sarenche (KU Leuven), Ertem Nusret Tas (Stanford University), Barnabé Monnot (Ethereum Foundation Research), Caspar Schwarz-Schilling (Ethereum Foundation Research), and Bart Preneel (KU Leuven)</i>	
Cryptographic Commitments on Anonymizable Data	527
<i>Xavier Bultel (INSA Centre Val de Loire, University of Orléans, Inria-Saclay, France), Céline Chevalier (Panthéon-Assas University, ENS, PSL University, CNRS, Inria, France), Charlène Jojon (INSA Centre Val de Loire, University of Orléans, Inria-Saclay, France), Diandian Liu (INSA Centre Val de Loire, University of Orléans, France), and Benjamin Nguyen (INSA Centre Val de Loire, University of Orléans, Inria-Saclay, France)</i>	
Cybersquatting in Web3:The Case of NFT	549
<i>Kai Ma (Huazhong University of Science and Technology, China), Ningyu He (The Hong Kong Polytechnic University, Hong Kong SAR, China), Jintao Huang (Huazhong University of Science and Technology, China), Bosi Zhang (Huazhong University of Science and Technology, China), Ping Wu (Fiberhome Telecommunication Technologies Co., Ltd., China), and Haoyu Wang (Huazhong University of Science and Technology, China)</i>	
Incompleteness in Number-Theoretic Transforms: New Tradeoffs and Faster Lattice Cryptography-Based Applications	565
<i>Syed Mahbub Hafiz (LG Electronics, USA), Bahattin Yildiz (LG Electronics, USA), Marcos A. Simplicio Jr (Universidade de São Paulo, Brazil), Thales B. Paiva (LG Electronics, USA), Henrique S. Ogawa (LG Electronics, USA), Gabrielle De Micheli (LG Electronics, USA), and Eduardo L. Cominetti (LG Electronics, USA)</i>	
Not in The Prophecies: Practical Attacks on Nostr	585
<i>Hayato Kimura (NICT / The University of Osaka), Ryoma Ito (NICT), Kazuhiko Minematsu (NEC / Yokohama National University), Shogo Shiraki (University of Hyogo), and Takanori Isobe (The University of Osaka)</i>	
Sandi: A System for Accountability	607
<i>F. Betül Durak (Microsoft Research, Redmond), Kim Laine (Microsoft Research, Redmond), Simon Langowski (MIT), and Radames Cruz Moreno (Microsoft Research, Redmond)</i>	
Sequentially Consistent Concurrent Encrypted Multimaps	631
<i>Archita Agarwal (MongoDB Research) and Zachary Espiritu (MongoDB Research)</i>	
The Art of Bonsai: How Well-Shaped Trees Improve the Communication Cost of MLS	655
<i>Céline Chevalier (Ecole normale supérieure, France - Paris-Panthéon-Assas University), Guirec Lebrun (Ecole normale supérieure, France - ANSSI, France), Ange Martinelli (ANSSI, France), and Jérôme Plût (ANSSI, France)</i>	

Network/Mobile

- Beneath the Surface: An Analysis of OEM Customizations on the Android TLS Protocol Stack . 677
Vinuri Bandara (IMDEA Networks Institute, Spain and Universidad Carlos III de Madrid, Spain), Stijn Pletinckx (University of California, Santa Barbara, CA, USA), Ilya Grishchenko (University of California, Santa Barbara, CA, USA), Christopher Kruegel (University of California, Santa Barbara, CA, USA), Giovanni Vigna (University of California, Santa Barbara, CA, USA), Juan Tapiador (Universidad Carlos III de Madrid, Spain), and Narseo Vallina-Rodriguez (IMDEA Networks Institute, Madrid, Spain)
- CAIBA: Multicast Source Authentication for CAN Through Reactive Bit Flipping 701
Eric Wagner (Fraunhofer FKIE & RWTH Aachen University), Frederik Basels (Fraunhofer FKIE), Jan Bauer (Fraunhofer FKIE), Till Zimmermann (Osnabrück University), Klaus Wehrle (RWTH Aachen University), and Martin Henze (RWTH Aachen University & Fraunhofer FKIE)
- Can You Hear Me? A First Study of VoIP Censorship Techniques in Saudi Arabia and the UAE 720
Friedemann Mattern (Max Planck Institute for Informatics, Germany), Anja Feldmann (Max Planck Institute for Informatics, Germany), and Devashish Gosain (Indian Institute of Technology Bombay, India)
- CovFUZZ: Coverage-based fuzzer for 4G&5G protocols 737
Ilja Siroš (KU Leuven, Belgium), Dave Singelee (KU Leuven, Belgium), and Bart Preneel (KU Leuven, Belgium)
- Endless Subscriptions: Open RAN is Open to RIC E2 Subscription Denial of Service Attacks 755
Felix Klement (University of Passau), Alessandro Brighente (University of Padova), Anup Kiran Bhattacharjee (Delft University of Technology), Stefano Ceconello (University of Padova), Fernando Kuipers (Delft University of Technology), Georgios Smaragdakis (Delft University of Technology), Mauro Conti (University of Padova), and Stefan Katzenbeisser (University of Passau)
- O'MINE: A Novel Collaborative DDoS Detection Mechanism for Programmable Data-Planes .. 771
Enkeleda Bardhi (Delft University of Technology), Chenxing Ji (Delft University of Technology), Ali Imran (University of Michigan), Muhammad Shahbaz (University of Michigan), Riccardo Lazzeretti (Sapienza University of Rome), Mauro Conti (University of Padua), and Fernando Kuipers (Delft University of Technology)
- SoK: Hardening Techniques in the Mobile Ecosystem – Are We There Yet? 789
Magdalena Steinböck (TU Wien), Jens Troost (VU Amsterdam), Wilco van Beijnum (University of Twente), Jan Serebinski (VU Amsterdam), Herbert Bos (VU Amsterdam), Martina Lindorfer (TU Wien), and Andrea Continella (University of Twente)
- The Danger of Packet Length Leakage: Off-path TCP/IP Hijacking Attacks Against Wireless and Mobile Networks 807
Guancheng Li (Tencent Security Xuanwu Lab, China), Minghao Zhang (Tsinghua University, China), Jianjun Chen (Tsinghua University, China), Ge Dai (Tencent Security Xuanwu Lab, China), Pinji Chen (Tsinghua University, China), Huiming Liu (Tencent Security Xuanwu Lab, China), Yang Yu (Tencent Security Xuanwu Lab, China), Haixin Duan (Tsinghua University, China), and Zhiyun Qian (University of California, Riverside, USA)

Crypto/ML

A Formal Security Analysis of Hyperledger AnonCreds	822
<i>Ashley Fraser (Lancaster University) and Steve Schneider (University of Surrey)</i>	
Efficient Authentication Protocols from the Restricted Syndrome Decoding Problem	845
<i>Thomas Johansson (Lund University), Mustafa Khairallah (Nanyang Technological University), and Vu Nguyen (Lund University)</i>	
Shaking up authenticated encryption	861
<i>Joan Daemen (Radboud University, Nijmegen, The Netherlands), Seth Hoffert (Nebraska, USA), Silvia Mella (Radboud University, Nijmegen, The Netherlands), Gilles Van Assche (STMicroelectronics, Diegem, Belgium), and Ronny Van Keer (STMicroelectronics, Diegem, Belgium)</i>	
SoK: Systematization and Benchmarking of Deepfake Detectors in a Unified Framework	883
<i>Binh M. Le (Sungkyunkwan University, South Korea), Jiwon Kim (Sungkyunkwan University, South Korea), Simon S. Woo (Sungkyunkwan University, South Korea), Kristen Moore (CSIRO's Data61, Australia), Alsharif Abuadbba (CSIRO's Data61, Australia), and Shahroz Tariq (CSIRO's Data61, Australia)</i>	
SPARK: Secure Privacy-Preserving Anonymous Swarm Attestation for In-Vehicle Networks ...	903
<i>Wouter Hellekens (KU Leuven, Belgium), Nada El Kassem (University of Surrey, United Kingdom), Md Masoom Rabbani (Chalmers University of Technology, Sweden), Edlira Dushku (Aalborg University, Denmark), Liqun Chen (University of Surrey, United Kingdom), An Braeken (Vrije Universiteit Brussel, Belgium), Bart Preneel (KU Leuven, Belgium), and Nele Mentens (KU Leuven, Belgium)</i>	
CTINexus: Automatic Cyber Threat Intelligence Knowledge Graph Construction Using Large Language Models	923
<i>Yutong Cheng (Virginia Tech), Osama Bajaber (Virginia Tech), Saimon Amanuel Tsegai (Virginia Tech), Dawn Song (UC Berkeley), and Peng Gao (Virginia Tech)</i>	
Deep Unlearn: Benchmarking Machine Unlearning for Image Classification	939
<i>Xavier Cadet (Imperial College London, United Kingdom), Anastasia Borovykh (Imperial College London, United Kingdom), Mohammad Malekzadeh (Nokia Bell Labs, United Kingdom), Sara Ahmadi-Abhari (Imperial College London, United Kingdom), and Hamed Haddadi (Imperial College London, United Kingdom)</i>	
LLMPot: Dynamically Configured LLM-based Honey-pot for Industrial Protocol and Physical Process Emulation	963
<i>Christoforos Vasilatos (New York University Abu Dhabi), Dunia J. Mahboobeh (New York University Abu Dhabi), Hithem Lamri (New York University Abu Dhabi), Manaar Alaam (New York University Abu Dhabi), and Michail Maniatakos (New York University Abu Dhabi)</i>	
On the Lack of Robustness of Binary Function Similarity Systems	980
<i>Gianluca Capozzi (Sapienza University of Rome), Tong Tang (The State Key Laboratory of Blockchain and Data Security, Zhejiang University), Jie Wan (The State Key Laboratory of Blockchain and Data Security, Zhejiang University), Ziqi Yang (The State Key Laboratory of Blockchain and Data Security, Zhejiang University - Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security), Daniele Cono D'Elia (Sapienza University of Rome), Giuseppe Antonio Di Luna (Sapienza University of Rome), Lorenzo Cavallaro (University College London), and Leonardo Querzoni (Sapienza University of Rome)</i>	

Harmless Backdoor-based Client-side Watermarking in Federated Learning	1002
<i>Kaijing Luo (Huawei Cloud, China) and Ka-Ho Chow (The University of Hong Kong, China)</i>	

Hardware/Systems

AceCov: Auxiliary Composite Edge Coverage for Fuzzing	1021
<i>Haruki Yoshida (The University of Tokyo), Yuichi Sugiyama (The University of Tokyo), and Ryota Shioya (The University of Tokyo)</i>	
CTRAPS: CTAP Client Impersonation and API Confusion on FIDO2	1034
<i>Marco Casagrande (EURECOM, France) and Daniele Antonioli (EURECOM, France)</i>	
Divide and Conquer: Introducing Partial Multi-Variant Execution	1049
<i>Jonas Vinck (KU Leuven, Belgium), Adriaan Jacobs (KU Leuven, Belgium), Alexios Voulimeneas (TU Delft, The Netherlands), and Stijn Volckaert (KU Leuven, Belgium)</i>	
LEAPFROG: The Rowhammer Instruction Skip Attack	1067
<i>Andrew Adiletta (MITRE), Caner M. Tol (WPI), Berk Sunar (WPI), Kemal Derya (WPI), and Saad Islam (WPI)</i>	
LegoLog: A configurable transparency log	1082
<i>Vivian Fang (UC Berkeley), Emma Dauterman (MIT and Stanford), Akshay Ravoor (UC Berkeley), Akshit Dewan (UC Berkeley), and Raluca Ada Popa (UC Berkeley)</i>	
openIPE: An Extensible Memory Isolation Framework for Microcontrollers	1104
<i>Marton Bognar (DistriNet, KU Leuven, Belgium) and Jo Van Bulck (DistriNet, KU Leuven, Belgium)</i>	
Pfuzzer: Practical, Sound, and Effective Multi-path Analysis of Environment-sensitive Malware with Coverage-guided Fuzzing	1121
<i>Nicola Bottura (Sapienza University of Rome, Italy), Daniele Cono D'Elia (Sapienza University of Rome, Italy), and Leonardo Querzoni (Sapienza University of Rome, Italy)</i>	
Mario: Multi-round Multiple-Aggregator Secure Aggregation with Robustness against Malicious Actors	1140
<i>Truong Son Nguyen (Arizona State University), Tancrede Lepoint (Amazon Web Services Inc), and Ni Trieu (Arizona State University)</i>	

Author Index