2026 IEEE 11th European Symposium on Security and Privacy (EuroS&P 2026)

Lisbon, Portugal
6-10 July 2026

Pages 1–752

IEEE Catalog Number: CFP26C75-POD
ISBN: 979-8-3195-1075-4

Copyright © 2026, IEEE

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:	CFP26C75-POD
ISBN (Print-On-Demand):	979-8-3195-1075-4
ISBN (Online):	979-8-3195-1074-7
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



TABLE OF CONTENTS

Security of NIST SP800-90A Hash-based DRBGs in the Seedless Model 1
Woohyuk Chung, Byeonghak Lee, Seongha Hwang, Seongkwang Kim, Jooyoung Lee

SoK: The Engineer's Guide to Post-Quantum Cryptography for Embedded Devices 23
Nikolai Puch, Maximilian Pursche, Sebastian N. Peters, Michael P. Heinl

Adaptor Multi-Signatures: Definition, Applications and Construction from Cryptographic Group Actions 43
Xuan Thanh Khuc, Willy Susilo, Dung Hoang Duong, Yannan Li, Partha Sarathi Roy, Kazuhide Fukushima Shinsaku Kiyomoto

Certificateless Key Exchange in QROM: Group-Action-based Construction and Performance 61
Li Duan, Yong Li, Joao Sobral

Privacy at your Fingertips: Enabling Rapid Client-Side Operations in Fully Homomorphic Encryption 78
Aikata Aikata, Florian Krieger, Sujoy Sinha Roy

SUMMER: Recursive Zero-Knowledge Proofs for Scalable RNN Training 99
Yuange Li, Xiong Fan

Breaking ECDSA with Electromagnetic Side-Channel Attacks: Challenges and Practicality on Modern Smartphones 118
Felix Oberhansl, Marc Schink, Nisha Jacob Kabakci, Michael Gruber, Dominik Klein, Sven Freud Tobias Damm, Michael Hartmeier, Ivan Gavrilan, Silvan Streit, Jonas Stappenbeck, Andreas Zankl

Bandwidth Efficient Partial Authorized PSI 138
Tjitske Koster, Francesca Falzon, Evangelia Anna Markatou

BiSON: Billion-Scale Oblivious Nearest-Neighbor Search in Milliseconds 160
Sankha Das, Rohan Ravi, Nishanth Chandran, Divya Gupta

SCOUT-CT: Sound Constant-Time Outcome with Uncertainty Tracking using multi-taint analysis 173
Damien Maier, Jean-François Pasche, Maxim Golay, Alexandre Duc

Helltrap: Transforming physical machines into UEFI rootkit traps 193
Darius Suciu, Jake Christensen, Radu Sion

UEFI Memory Forensics: A Framework for UEFI Threat Analysis 208
Kalanit Suzan Segal, Hadar Cochavi Gorelik, Oleg Brodt, Yuval Elbahar, Yuval Elovici, Asaf Shabtai

Rethinking Human Biometric Security Under Behavioral Copy and Robot Replay 225
Zeyu Deng, Zhen Meng, Long Huang, Yichi Zhang, Jingwei Zhang, Chen Wang, Emma Li, Philip G. Zhao

I can't recognize (yet): Delayed Rendering to Defeat Visual Phishing Detectors 242
Ying Yuan, Cristiano Alex Rado, Giovanni Apruzzese, Mauro Conti, Luigi Vincenzo Mancini

Dealing with Digital Risks: Online Security, Safety, and Privacy Advice provided to Children by Peers, Parents, and Teachers 261
Alexander Löbel, Andreas Klinger, Frederic Salmen, Clemens Bönnen, Ulrike Meyer

SoK: The Next Frontier in AV Security: Systematizing Perception Attacks and the Emerging Threat of Multi-Sensor Fusion 281
Shahriar Rahman Khan, Tariqul Islam, Raiful Hasan

ViNET: Connecting the Unconnected using Video over LTE 301
Manav Mittal, Yogesh Kaushik, Anirudh S Kumar, Mukulika Maity, Sambuddho Chakravarty

SoK: Cybersecurity Assessment of Humanoid Ecosystem 319
Priyanka Prakash Surve, Asaf Shabtai, Yuval Elovici

SoK: The Cyber Attack Surface of Unmanned Vehicles (UxVs) 341
Alessandro Cantelli-Forti, Hosam Alamleh

Quantifying Memory Cells Vulnerability for DRAM Security 364
Zilong Hu, Hongming Fei, Prosanta Gope, Jack Miskelly, Owen Millwood, Biplab Sikdar

Practical Attacks on Session Messenger and Oxen Blockchain 378
Tingfeng Yu, Thomas Haines

PROF: Protected Order Flow in a Profit-Seeking World 398
Kushal Babel, Nerla Jean-Louis, Yan Ji, Ujval Misra, Mahimna Kelkar, Kosala Yapa Mudiyanselage Andrew Miller, Ari Juels

Persistent BitTorrent Trackers 419
François-Xavier Wicht, Zhengwei Tong, Shunfan Zhou, Hang Yin, Aviv Yaish

Decentralized Reliability Estimation for Low-Latency Mixnets 436
Claudia Diaz, Harry Halpin, Aggelos Kiayias

ANARKey: A New Approach to (Socially) Recover Keys 455
Aniket Kate, Pratyay Mukherjee, Hamza Saleem, Pratik Sarkar, Bhaskar Roberts

Verifying Account Ecosystems With Graph Transformations 470
Freya Murphy, Saša Radomirović

Honest Users Make Honest Mistakes: A Framework for Analysing eID Protocols 491
Ole Martin Edstrøm, Kristian Gjøsteen, Hans Heum, Sjouke Mauw, Felix Stutz

Formal Security Analysis of Swedish BankID 505
Qinghua Wang

All You Need is Trust: A Longitudinal Analysis of Italy's OpenID Federation Journey 518
Tobias Hilbig, Erwin Kupris, Thomas Schreck

Implementing and Evaluating the Usability of Reliable Voter Complaints in E2E Verifiable Remote Electronic Voting 536
Tobias Hilt, Christian Mack, Philipp Matheis, Benjamin Berens, Tobias Länge, Rolf Haenni, Reto E. Koenig Philipp Locher, Melanie Volkamer

From Beats to Breaches: How Offensive AI Infers Sensitive User Information from Playlists 558
Stefano Cecconello, Mauro Conti, Luca Pajola, Luca Pasa, Pier Paolo Tricomi

Revisiting Privacy Leakage in Machine Unlearning: Membership Inference Beyond the Forgotten Set 571
Jie Fu, Nima Naderloui, Da Zhong, Yuan Hong, Wendy Hui Wang

GDBR: Label Recovery Attack Against Partial Gradient Encryption in Federated Learning 592
Rui Zhang, Ka-Ho Chow

Federated Matrix Factorization under Local Differential Privacy via Directional Noise 608
Nawfal Abbassi Saber, Loubna Mekouar, Youssef Iraqi

Covert Attacks on Machine Learning Training in Passively Secure MPC 620
Matthew Jagielski, Rahul Rachuri, Peter Scholl, Daniel Escudero

Auditing Fairness-Privacy Trade-offs: Subpopulation-Level Effects of Fairness-Enhancing Algorithms 634
Umid Suleymanov, Ilhama Novruzova, Khalid Mammadov, Natavan Hasanova, Murat Kantarcioglu

Security-by-Design for LLM-Based Code Generation: Leveraging Internal Representations for Concept-Driven Steering Mechanisms 658
Maximilian Wendlinger, Daniel Kowatsch, Konstantin Böttinger, Philip Sperl

SecDTD: Dynamic Token Drop for Secure Transformers Inference 679
Yifei Cai, Zhuoran Li, Yizhou Feng, Qiao Zhang, Hongyi Wu, Danella Zhao, Chunsheng Xin

Re-Key-Free, Risky-Free: Adaptable Model Usage Control 696
Zihan Wang, Zhongkui Ma, Xinguo Feng, Chuan Yan, Dongge Liu, Ruoxi Sun, Derui Wang, Minhui Xue Guangdong Bai

Aggressive, Imperceptible, or Both: Architecture-Aware Hybrid Byzantines in Federated Learning 712
Emre Özfatura, Kerem Özfatura, Baturalp Büyükateş, Mert Coşkuner, Alptekin Küpçü, Deniz Gündüz

Cross-Host Lateral Movement Attacks Detection with QUIC-Aware Dynamic Information Flow Tracking 736
Kokthay Poeng, Laurent Schumacher

Abusing Cloud Services to Establish Covert Channels in Secure Enterprise Environments 753
Kotaiba Alachkar, Eduardo Barbaro, Cristiano Giuffrida, Michel van Eeten, Yury Zhauniarovich

Tyche: Composable Isolation as a Foundation to Manage Trust in the Cloud 772
Adrien Ghosn, Charly Castes, Neelu S. Kalani, Yuchen Qian, Marios Kogias, Edouard Bugnion

CAEC: Confidential, Attestable, and Efficient Inter-CVM Communication with Arm CCA 789
Sina Abdollahi, Amir Al Sadi, David Kotz, Marios Kogias, Hamed Haddadi

DNS Trap: Unveiling Reactive DNS Monitoring via Stimulated Network Emissions 804
Aaron Faulkenberry, Athanasios Avgetidis, Omar Alrawi, Zane Ma, Roberto Perdisci, Manos Antonakakis

SourceFabric: Consistent and Scalable Security Policies for Git Repositories 820
Aditya Sirish A Yelgundhalli, Patrick Zielinski, Marcela S. Melara, Dennis Roellke, Reza Curtmola Justin Cappos

SoK: A Defense-Oriented Evaluation of Software Supply Chain Security 836
Eman Abu Ishgair, Juanita Gomez, Marcela S. Melara, Alvaro Cardenas, Santiago Torres-Arias

ARVO: Atlas of Reproducible Vulnerabilities for Open-Source Software 860
Xiang Mei, Jordi Del Castillo, Pulkit Singh Singaria, Haoran Xi, Abdelouahab Benchikh, Tiffany Bao Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, Hammond Pearce, Brendan Dolan-Gavitt

Towards Multi-Stakeholder Vulnerability Notifications in the Ad-Tech Supply Chain 874
Yash Vekaria, Rishab Nithyanand, Zubair Shafiq

VerIFI: Formal Verification of Microarchitectural Information-Flow Integrity 892
Katharina Ceesay-Seitz, Flavien Solt, Mengyuan Yin, Kaveh Razavi

SoK: Honeypots & LLMs, More Than the Sum of Their Parts? 910
Robert A. Bridges, Thomas R. Mitchell, Mauricio Muñoz, Ted Henriksson

KNOWML: Improving Generalization of ML-NIDS with Attack Knowledge Graphs 929
Xin Fan Guo, Xinran Zheng, Albert Merono Penuela, Lorenzo Cavallaro, Sergio Maffeis, Fabio Pierazzi

GRAAL: GRAph-based Analysis of Logs for Advanced AI-based Intrusion Detection Systems 949
Fanny Dijoud, Pierre-François Gimenez, Michel Hurfin, Frédéric Majorczyk, Barbara Pilastre

PHASE: Passive Human Activity Simulation Evaluation 971
Steven Lamp, Jason D. Hiser, Anh Nguyen-Tuong, Jack W. Davidson

Automated Stealthy Wear-Out Attack on Digital Twins With Deep Reinforcement Learning 988
Joshua Haworth, Aryan Pasikhani, George Pavlides, Prosanta Gope, John Clark

SoK: A Taxonomy for Cybersecurity Incident Response Influence Factors 1005
Thomas Biege, Marius Brockhoff, Jonas Kaspereit, Fabian Ising, Lea Gröber, Sebastian Schinzel

Measuring Healthcare Data Leaks and Security Flaws at Internet Scale 1027
Nico Brüggemann, Lukas Schmidt, Marvin Dölzer, Marius Brockhoff, Fabian Ising, Christoph Saatjohann Sebastian Schinzel

"Security vs. Interoperability" Arguments: An Analytical Framework 1046
Daji Landis, Elettra Bietti, Sunoo Park

One Space To Match Them All: Template Inversion and Impersonation under Realistic Post-Breach Conditions 1065
Willem Verheyen, Tim Van Hamme, Davy Preuveneers, Wouter Joosen

A Critical Look at Accelerometer-Based Driver Fingerprinting: Between Deceptive Physics, Sensor Mingling and Weak Multiclass Assumptions 1082
Bogdan Groza, Emilia Caragea, Adriana Berdich, Camil Jichici

The Unbearable Randomness of Fuzzing 1102
Dongjia Zhang, Romain Malmain, Andrea Oliveri, Davide Balzarotti, Aurélien Francillon

SoK: A Systematic Review of Integration and Reproducibility of Fuzzing Research into AFL++ 1117
Nico Schiller, Nils Bars, Moritz Schloegel, Thorsten Holz

It’s Not You, It’s Me: Reevaluating the Relationship between Concolic Execution and Fuzzing 1137
Lukas Dresel, Stijn Pletinckx, Fabio Gritti, Mathias Payer, Giovanni Vigna, Christopher Kruegel

Themis: Context-Aware Grey-box Fuzzing for WordPress Plugins 1160
Matteo Leonelli, David Jannis Dewes, Thorsten Holz

SandVenture: Escaping JavaScript Sandboxes with Objective-driven Input Generation 1180
Mingi Jung, Hyeon Heo, Seongil Wi

High Impedance: Analysis of Publicly Disclosed Vulnerabilities in FPGA IP Cores 1198
Imtiaj A. Chowdhury, Eric Ackermann, Sven Bugiel

Scribe: Practical Static Binary Patching via Binary-Aware Recompilation of Decompiled Code 1218
Han Dai, Soumyakant Priyadarshan, Abdullah Imran, Ruoyu Wang, Antonio Bianchi

Match & Mend: Minimally Invasive Local Reassembly for Patching N-day Vulnerabilities in ARM Binaries 1235
Sebastian Jänich, Merlin Sievers, Johannes Kinder

Attacking the First-Principle: A Black-Box Query-Free Targeted Mimicry Attack on Binary Function Classifiers 1251
Gabriel Sauger, Jean-Yves Marion, Sazzadur Rahaman, Victor Matrat, Vincent Tourneur, Muaz Ali

Towards Deployable VCFI: Architectural Analysis and Cache-Optimized Verification 1273
Pinghai Yuan, Hao Jiang, Zhixiang Lu, Fulong Chen, Zhenjiang Qian

StreamCFI: Streamed Per-Input Control-Flow Integrity 1285
Konstantinos Kleftogiorgos, Cristiano Giuffrida, Georgios Portokalidis

MARISSA: Efficient Inference of Network Protocols using Similarity Digest Clustering and Multiple Sequence Algorithms 1299
Pablo Ruiz-Lezcano, Daniel Uroz, Ricardo J. Rodríguez

Agility for Steganalysis: Dealing with Distribution Drift in JPEG File Structures 1313
Matěj Zorek, Tomáš Pevný, Rainer Böhme

ADVISE: Adversarial Invisible Steganography for Event-data 1326
Aaditya Arunkumar Khant, Raveen Wijewickrama, Murtuza Jadliwala

The Coding Limits of Robust Watermarking for Generative Models 1343
Danilo Francati, Yevin Nikhel Goonatilake, Shubham Vivek Pawar, Daniele Venturi, Giuseppe Ateniese

Formal Foundations of Trigger-Based Watermarking 1357
Stefano Calzavara, Lorenzo Cazzaro, Claudio Lucchese, Salvatore Orlando

The Clone Strikes Back: Efficient Vulnerable Code Detection in Custom Android-based Systems 1376
Esteban Luques, Carlo Mazzocca, Güliz Seray Tuncay, Selcuk Uluagac

Investigating Developers' Usage and Perception of Trusted Execution Environment Features in Android 1394
Abdullah Imran, Güliz Seray Tuncay, René Mayrhofer, Antonio Bianchi

The Invisible Ink of the Android Malware World: A Longitudinal Study on the Usage of Covert Communication Channels 1415
Zeya Umayya, Manan Aggarwal, Manan Chugh, Mann Nariya, Yogesh Kaushik, Sambuddho Chakravarty

Unidentifiable Identifier: Attacking Bluetooth Applications with Duplicated UUIDs 1436
Siyu Shen, Yi Chen, Fenghao Xu, Shuaike Dong, Wenrui Diao, Di Tang, Kehuan Zhang

SoK: Understanding the state of IoT-specific vulnerabilities via CVE characterization with LLIoT 1453
Tina Rezaei, Suzan Bayhan, Andrea Continella, Jeroen Van Der Ham-De Vos, Roland Van Rijswijk-Deij

Secrets Best Not Shared: DNS Privacy Enhancements for the Constrained IoT 1475
Martine S. Lenders, Thomas C. Schmidt, Matthias Wählisch