2026 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2026)

Lisbon, Portugal
6-10 July 2026

IEEE Catalog Number: CFP26N35-POD
ISBN: 979-8-3195-2259-7

IEEE
Advancing Technology for Humanity

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:	CFP26N35-POD
ISBN (Print-On-Demand):	979-8-3195-2259-7
ISBN (Online):	979-8-3195-2258-0
ISSN:	2768-0649

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

The Interlocutor Effect: Why LLMs Leak More Personal Data to Agents Than Humans 1
Faouzi El Yagoubi, Godwin Badu-Marfo, Ranwa Al Mallah

Addressing Labelled Data Scarcity: Taxonomy-Agnostic Annotation of PII Values in HTTP Traffic using LLMs 6
Thomas Cory, Axel Küpper

Can We Explain What We Anonymize? On the Impact of Data Anonymization on Post-hoc Model Explanations 20
Casper Lauge Nørup Koch, Mina Alishahi, Gaurav Choudhary

ASTIV: A Classification Framework for Privacy-Respecting WiFi Sensing 29
Kilian Osenstätter, Erik Krempel

Location Privacy Protection through Road Network Adaptability and User Mobility Prediction 38
Lara Santos, Mariana Cunha, João P. Vilela

PEMM: A Privacy Engineering Maturity Model 47
Andreas M. Binder, Immanuel Kunz

Alohomora! Facilitating Personal Data Access Through Automated Graph Extraction and Integration 56
Nicola Leschke, Karl Wolf, Frank Pallas

Trading Latency for Privacy: Mixnet Usability for Email and Instant Messaging 65
Harry Halpin, Daniel Nemet

The Hacker's Guide to Staying Out of Jail: Examining Prevention of Prosecution Content on the Dark Web 72
Emerson Suter, Matthew Edwards

Analyzing Supply and Demand Signals for Cybercrime Services in Technical-Support Scams 83
Raghavendra Cherupalli, Yi Ting Chua, Tyler Moore, Gary Warner

Topical Shifts in the Dark Web: A Longitudinal Analysis of Content from the Cybercrime Ecosystem 93
Roy Ricaldi, Maximilian Schäfer, Philipp Zech, Luca Allodi, Raffaela Groner, Irdin Pekaric

From Cyber Threat to Political Action: The Identity and Motivations Presented by Anonymous Sudan for DDoS Attacks 108
Catherine Lowery, Matthew Edwards, Laura G. E. Smith

From Forum Threads to Cyber Threats: How Hackers Discuss Human Factors 120
Jan-Philip van Acken, Marre Slikker, Slinger Jansen, Katsiaryna Labunets

Towards Group-level Cybercriminal Profiling - Cultural Dimensions and Participation Roles in Dark Web Communities 138
Elizabeth Eardley, Simran Chandarana, Konstantinos Mersinas

An Assessment of Geopolitical Discussions in Cybercrime Forums 151
Isa-May Beauchamp, Estelle Ruellan, Masarah Paquet-Clouston

Large-Scale Analysis of Malware Distribution via Fake Game Cheats and Cracked Software on YouTube 161
Rei Yamagishi, Shota Fujii, Tatsuya Mori

Tor Through the Lens of OSINT: Studying the Presence of Exit Nodes in Blocklists 169
Adrián Jiménez-Gamo, Sergio Pastrana

Work in Progress: An Analysis of ATT&CK TTP Adoption and Semantic Ambiguity 181
Manuel Suarez-Roman, Juan Caballero, Juan Tapiador

Graph-Based Modelling and Prediction of Adversary Behaviour from Honeypot Traces 187
David Guilherme, Miguel Faísco, Hans P. Reiser, Ibéria Medeiros

Connecting the Dots using Digital Fingerprints: Ontology-Grounded Action-Centric Knowledge Graphs for Scalable Cybercrime Case Linkage 195
Spriha Joshi, Anna Wilbik, Frank Thuijsman

It Works on My Machine: A Systematization of Knowledge on Reproducibility and Replicability in ML-Based Ransomware Detection 209
Bruno Pereira, Beatriz Cepa, Cláudia Brito, João Marco Silva, Vera Rimmer, João Paulo, Tânia Esteves

Analyzing Chain of Thought (CoT) Approaches in Control Flow Code Deobfuscation Tasks 221
Seyedreza Mohseni, Sarvesh Baskar, Edward Raff, Manas Gaur

Towards Improved Anomaly Detection for Cloud Cybersecurity via Graph Neural Networks 233
Manu Nandan, Tj Jaymes, Michael Brautbar, Edward Raff

Cybersecurity is the True Frontier for Generative AI Success or Failure 242
Edward Raff, Maor Ashkenazi, Sagar Samtani, David J. Elkind, Sven Krasser

Adversarial Malware Can Be Both Evasive and Deceiving: a Gradient-based Attack Against Prediction and Explainability in Windows PE Malware Detection 253
Luca Lobascio, Giuseppina Andresini, Annalisa Appice, Donato Malerba

Contamination-Robust Anomaly Detection under Weak Supervision with Explainable Representations 262
Guowei Wu, Huanqi Tu, Xuyun Zhang, Lin Yao

XplainCVSS: Interpretable Machine Learning for Explainable CVSS Vulnerability Severity Prediction 270
Christopher Beddies, Stefan Kubica, Bernd Heimer, Bernd Eylert

Towards Explaining Classification Models in Security with Sparse Autoencoders 278
Nils Ole Breuer, Lorenz Linhardt, Philipp Normann, Daniel Arp

CyberGuardEV: Interoperable Non-Intrusive IDS for Electric Vehicle Charging Stations 290
A. Brighente, N. Borgioli, D. Capriglione, M. Conti, D. Donadel, G. Miele, L. Tari

Security risk assessment in distributed systems made practical: Application to a real-world mobility system 298
Maike Massierer, Carsten Nobbe

Revisiting Bluetooth Vulnerabilities in Automotive Infotainment Systems: A Remote Code Execution Case Study 308
Philippe Trébuchet, Guillaume Bouffard

Sensor Forensics in Autonomous Vehicles: Requirements, Challenges, and Evaluation via LiDAR Attack Simulation 316
Masashi Fukunaga, Takeshi Sugawara

CAN We Trust Your Results? A Cross-Dataset Study of Automotive IDS Evaluation 327
Beatrix Koltai, Gergely Ács, András Gazdag

Adversarial Weather For Improving Robustness of Traffic Sign Classification 341
Aliza Katharina Reif, Oscar Hernán Ramírez-Agudelo, Michael Karl

IRIS: Invisible Laser Injection for Stealthy Backdoor Attacks 352
Yuta Soga, Daisuke Kosuge, Taiga Manabe, Naoto Yanai, Hiroshi Yamamoto, Yoshihisa Takayama Toshihiro Ohigashi

Improving Memory Efficiency of NIST Post-Quantum Cryptography for Microcontrollers 359
Dominik Marchsreiter, Holger Kinkelin, Und Georg Carle

Revisiting the ETSI ITS Lifecycle with Certificateless Authorization Based on Group Signatures 371
Riccardo Gennaro, Stefano Berlato, Alessandro Tomasi, Silvio Ranise, Florian Hahn

Analyzing the Unlinkability of SD-JWT: A Machine Learning Perspective 385
Zahra Ebadi Ansaroudi, Alessandro Tomasi, Francesco Antonio Marino, Silvio Ranise

Comparison of Private Key Protection Techniques for Digital Identity Wallets 396
Jelizaveta Vakarjuk, Alisa Pankova, Aivo Kalu

Risk Management Framework for LLM-Enabled Identity Tools: Mapping OWASP LLM Top 10 to NIST CSF 2.0 413
Sanaa S. Mironov, Shahmir Rizvi, Behnam Shariati

Towards a Risk-Cost Model for Financial Adaptive Authentication 424
Supriya Khadka, Sanchari Das

Correlation-Aware Probe Planning for Cloud Identity Attack Paths 432
Eric Conklin

Authenticating and Authorizing the Caller: A Defense Mechanism Against Caller ID Spoofing 438
Salem Wollel, Sanna Suoranta, Otto Seppälä