2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2025)

Venice, Italy
30 June - 4 July 2025

IEEE Catalog Number: CFP25N35-POD
ISBN: 979-8-3315-9547-0

IEEE
Advancing Technology for Humanity

IEEE Catalog Number:	CFP25N35-POD
ISBN (Print-On-Demand):	979-8-3315-9547-0
ISBN (Online):	979-8-3315-9546-3

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

Mitigating Information Leakage in Large Language Models: Evaluating the Impact of Code Obfuscation on Vulnerability Detection 1
Bengü Gülay, Cemal Yılmaz

Admin/1423: On the Insecurity of Open-Source 5G Core Network Deployments in the Wild 9
Katharina Kohls

Bypassing Audio reCAPTCHA with Automatic Speech Recognition Models 14
Paul Aubry, Juliette Devoivre, Damien Carron, Simon Fernandez, Andrzej Duda, Maciej Korczyński

Demystifying the Role of Rule-Based Detection in AI Systems for Windows Malware Detection 19
Andrea Ponte, Luca Demetrio, Luca Oneto, Ivan Tesfai Ogbu, Battista Biggio, Fabio Roli

On the Effect of Ruleset Tuning and Data Imbalance on Explainable Network Security Alert Classifications: A Case-Study on DeepCASE 26
Koen T. W. Teuwen, Sam Baggen, Emmanuele Zambon, Luca Allodi

Democratizing Generic Malware Unpacking 40
Thorsten Jenke, Max Ufer, Manuel Blatt, Leander Kohler, Elmar Padilla, Lilli Bruckschen

Toward Automatically Generating User-Specific Recovery Procedures After Windows Malware Infections 49
Jerre Starink, Cassie Wanjun Xu, Andrea Continella

A Unified Comparison of Tabular and Graph-Based Feature Representations in Machine Learning for Malware Detection 58
Samy Bettaieb, Serena Lucca, Charles-Henry Bertrand Van Ouytsel, Axel Legay, Etienne Rivière

Do Fear the REAPIR: Adversarial Malware from API Replacement 69
Luke Kurlandski, Rayan Mosli, Yin Pan, Sirapat Thianphan, Matthew Wright

CTI-HAL: A Human-Annotated Dataset for Cyber Threat Intelligence Analysis 79
Sofia Della Penna, Roberto Natella, Vittorio Orbinato, Lorenzo Parracino, Luciano Pianese

The Dark Side of the Web: Towards Understanding Various Data Sources in Cyber Threat Intelligence 89
Saskia Laura Schröer, Noè Canevascini, Irdin Pekaric, Philine Widmer, Pavel Laskov

Is this your USB? No, but Check this QR Code for a Free Meal! Assessing Awareness Against Dropped USBs and Malicious QR Codes 100
Johannes Nordskov, Tyge Tiessen, Emmanouil Vasilomanolakis

Decomposing Culture within Threat Actor Groups – Insights from the Conti Ransomware Collective 113
Konstantinos Mersinas, Aimee Liu, Niki Panteli

An Experimental Design to Investigate Attacker Actions on an Access-as-a-Service 'Criminal' Platform 119
Roy Ricaldi, Yasen Yalamov, Michele Campobasso, Luca Allodi, Hannah Kool, Asier Moneva E. Rutger Leukfeldt

Port in a Storm: Iranian Cyber Operations and Chinese Strategic Interests in Middle Eastern Maritime Infrastructure 125
Cosimo Melella, Francesco Ferazza, Konstantinos Mersinas, Ricardo Lugo

Yet Another Diminishing Spark: Low-Level Cyberattacks in the Israel-Gaza Conflict 136
Anh V. Vu, Alice Hutchings, Ross Anderson

LogoTrust: Leveraging BIMI to Build a Validated Dataset of Brands, Domain Names, and Logos 142
Youssef Abyaa, Olivier Hureau, Andrzej Duda, Maciej Korczyński

Hunting Review Bombs with BRIDGE - A Bipartite Graph Neural Network Approach to Abuse Detection 148
Gonzalo Sobarzo Abufon, Juan Vanerio, Javier Bustos-Jiménez, Pedro Casas

Intelligent Detection of Non-Essential IoT Traffic on the Home Gateway 157
Fabio Palmese, Anna Maria Mandalari, Hamed Haddadi, Alessandro E. C. Redondi

Early-Stage Anomaly Detection: A Study of Model Performance on Complete vs. Partial Flows 163
Adrian Pekar, Richard Jozsa

PPT-GNN: A Practical Pretrained Spatio-Temporal Graph Neural Network for Network Security 174
Louis Van Langendonck, Ismael Castell-Uroz, Pere Barlet-Ros

Tracing Vendors: A Middlebox-Centric Study of Network Interference 181
Bulut Ulukapi, Anna Sperotto, Ralph Holz

One Does Not Simply Score a Website: Evaluating Website Security Scoring Algorithms 192
Daan Vansteenhuyse, Victor Le Pochat, Gertjan Franken, Lieven Desmet

Drifting Away: A Cyber-Security Study of Internet-Exposed OPC UA Servers 200
Ricardo Yaben, Emmanouil Vasilomanolakis

RustiFlow: Bridging the Gap Between Security Research and Practice Using eBPF-Based Network Flow Extraction 208
Miel Verkerken, Matisse Callewaert, Laurens D'hooge, Tim Wauters, Bruno Volckaert, Filip De Turck

CFA-Bench: Cybersecurity Forensic Llm Agent Benchmark and Testing 222
Francesco De Santis, Kai Huang, Rodolfo Valentim, Danilo Giordano, Marco Mellia, Zied Ben Houidi Dario Rossi

From Cluttered to Clustered: Addressing Privacy Threat Explosion through Automated Clustering 231
Jonah Bellemans, Mario Raciti, Dimitri Van Landuyt, Laurens Sion, Giampaolo Bella, Lieven Desmet Wouter Joosen

Explaining and Visualizing Synthetic Data Quality Using Statistical Distances 242
Juko Yamamoto, Takayuki Miura, Rina Okada, Masanobu Kii, Atsunori Ichikawa

Identification of Compositional Risks in Data Protection Impact Assessments and Beyond 251
Henrik Graßhoff, Meiko Jensen, Malte Hansen, Nils Gruschka

Formguard: Continuous Privacy Testing for Websites Using Automated Interaction Replay 260
Tim Vlummens, Gunes Acar

Right Here, Right Now: User Perceptions of In-Place Contextual Privacy Options 269
Florian Dehling, Jan Tolsdorf, Luigi Lo Iacono

PILLAR: LINDDUN Privacy Threat Modeling Using LLMs 278
Majid Mollaeefar, Andrea Bissoli, Dimitri Van Landuyt, Silvio Ranise

Securing the Lane: Defences Against Patch Attacks on Autonomous Vehicle's Lane Detection 287
Romana Blazevic, Alexander Toch, Omar Veledar, Georg Macher

Stop! Camera Spoofing Via the in-Vehicle IP Network 296
Dror Peri, Avishai Wool

The Image Scaling Attack: Unveiling the Risks in Traffic Sign Classification 311
Aliza Reif, Tarek Stolz, Stjepan Picek, Oscar Hernán Ramírez-Agudelo, Michael Karl

WiP: Concept Drift Management in Edge-AI for Autonomous Vehicles 322
Rohit Ravichandran, Mahshid Mehr Nezhad, Carsten Maple

Self-Sovereign Identities for Software-Defined Vehicles 330
Christian Prehofer

CheckOCPP: Automatic OCPP Packet Dissection and Compliance Check 336
Soumaya Boussaha, Victor Fresno Gómez, Thomas Barber, Daniele Antonioli

Avatar: Adversarial Vehicle Trajectory Attack Targeting Autonomous Driving Planner 344
Jiadong Liu, Tatsuya Mori

Work in Progress: Leveraging Large Language Models for Cybersecurity Compliance: A Pilot Study in ISO 27001 Audit Planning 352
Ahmed Salman, Yara Alsiyat, Sadie Creese, Michael Goldsmith

Tap, Pay, and Worry: Users' Perceptions of Contactless Payment Attacks Versus Technical Feasibility 361
Mahshid Mehr-Nezhad, Maryam Mehrnezhad, Timur Yunusov, Feng Hao

Work in Progress: Artificial Intelligence in Cybersecurity - Developing a Framework for Ethically Responsible Practices 375
Nandshin Lehniger, Michael Kubach

Work in Progress: Secure Deletion on Cloud - a Constant Battle 382
Konstantina Fotari, François Dupressoir, Kopo Marvin Ramokapane

Understanding How Privacy and Data Protection Perceptions Shape Nigerian Journalists' Use of AI Tools: A Work in Progress 389
Oluwamayowa Tijani, Jamie Mahoney, Santosh Vijaykumar, James Nicholson

Work in Progress: Effects of Enforcing International Law on Cyber Conflict Using Wargaming 396
Aidan Marchildon, Ievgeniia Kuzminykh, Bogdan Ghita

An Early Experience With Confidential Computing Architecture for On-Device Model Protection 402
Sina Abdollahi, Mohammad Maheri, Sandra Siby, Marios Kogias, Hamed Haddadi

Proving Attributes About Confidential Compute Services with Validation and Endorsement Services 412
Anjo Vahldiek-Oberwagner, Marcela S. Melara

End-To-End Confidentiality with Sev-Snp Leveraging in-Memory Storage 415
Lorenzo Brescia, Iacopo Colonnelli, Valerio Schiavoni, Pascal Felber, Marco Aldinucci

Enclave Application Cache for RISC-V Keystone 423
Takumu Umezawa, Akihiro Saiki, Keiji Kimura

OPENCCA: An Open Framework to Enable Arm CCA Research 430
Andrin Bertschi, Shweta Shinde

Principled Symbolic Validation of Enclaves on Low-End Microcontrollers 436
Gert-Jan Goossens, Jo Van Bulck

Atlas: A Framework for ML Lifecycle Provenance & Transparency 449
Marcin Spoczynski, Marcela S. Melara, Sebastian Szyller

Wait a Cycle: Eroding Cryptographic Trust in Low-End Tees via Timing Side Channels 463
Ruben Van Dijck, Marton Bognar, Jo Van Bulck

Narrowing the Gap Between Tees Threat Model and Deployment Strategies 472
Filip Rezabek, Jonathan Passerat-Palmbach, Moe Mahhouk, Frieder Erdmann, Andrew Miller

Decentralised Supply Chain Reputation: A Privacy and Self-Sovereign Identity Perspective 475
Abubakar-Sadiq Shehu, Steve Schneider

Identity Threats and Where to Find Them: Mapping ITDR and MITRE ATT&CK 486
Vitali Serzantov, Erwin Kupris, Thomas Schreck

Replication Study: Cross-Country Evaluation of the Recognition-Based Graphical Authentication Scheme in AR and VR Environments 497
Naheem Noah, Peter Mayer, Sanchari Das

Security Requirements Classification by Means of Explainable Transformer Models 509
Luca Petrillo, Fabio Martinelli, Antonella Santone, Francesco Mercaldo

Towards Privacy-Preserving Revocation of Verifiable Credentials with Time-Flexibility 517
Francesco Buccafurri, Carmen Licciardi

HFuzz-Rb: Real-Time Roadblock Detection in Fuzz Testing 523
Subhojeet Mukherjee, Ritesh Kumar Kalle

A Review of Anti-Phishing Email Control Measures: Why we Need a Novel Digital Signature Scheme 531
Ye Li, Abu Barkat Ullah, Dat Tran, Elisa Martinez Marroquin, Wanli Ma

Are You Sure That is Secure? Assessing Organizations Security Readiness Via a Devsecops Maturity Model 539
Alessandro Brighente, Elisa Burato, Mauro Conti

Sok: Zero Trust as a Strategy to Address Devsecops Challenges 547
Anita Nair, Serena Nicolazzo, Antonino Nocera, Rafidha Rehiman K. A., Vinod P.

Towards Continuous Risk Assessment and Conformance Checking of IdM Deployments 556
Andrea Bisegna, Roberto Carbone, Laura Cristiano, Pietro De Matteis, Silvio Ranise

Concept for Designing an ICS Testbed from a Penetration Testing Perspective 562
Sebastian Kraust, Peter Heller, Jürgen Mottok

The OWApp Benchmark: An OWASP-Compliant Vulnerable Android App Dataset 570
Luca Ferrari, Franceso Pagano, Luca Verderame, Alessio Merlo

Covert BLE Data Exfiltration via Apple's Find My Network: A Malware Prototype and Defense Strategies 582
Hosam Alamleh, Alessandro Cantelli-Forti

Real-World Study of the Security of Educational Test Systems 589
Stefan Gast, Sebastian Daniel Felix, Alexander Steinmaurer, Jonas Juffinger, Daniel Gruss

Statistical Evaluation of Entropy Accumulation in Linux 601
Alexandre Bouez, Joan Daemen, Bart Mennink

Work-in-Progress: Optimizing Performance of User Revocation in Cryptographic Access Control with Trusted Execution Environments 614
Ion Andy Ditu, Stefano Berlato, Matteo Busi, Roberto Carbone, Silvio Ranise

From Edge to Cloud: Securing Distributed Containerized Applications 620
Luca Verderame, Giorgia Bolognesi, Enrico Pezzano, Massimiliano Rak, Alberto Falcone
Giacomo Benedetti, Massimo Guarascio, Luca Caviglione, Roberto Carbone, Roberto Doriguzzi-Corin
Maurizio Giacobbe, Giovanni Merlino, Antonio Puliafito, Massimiliano Baldo, Marino Miculan
Vincenzo Riccio, Massimo Ficco

Cognitive Biases in Cyber Attacker Decision Making: Translating Behavioral Insights Into Cybersecurity 631
Anu Aggarwal, Maria Jos Ferreira, Palvi Aggarwal, Prashanth Rajivan, Cleotilde Gonzalez

Towards Bio-Inspired Cyber-Deception: A Case Study of SSH and Telnet Honeypots 647
Anastasia Safargalieva, Emmanouil Vasilomanolakis

Experience Paper: Uncovering a Privileged Insider Threat in Action 657
Raj Gopalakrishna, Rajaram Bhaskaran

Position Paper: The Extended Pyramid of Pain: The Attacker's Nightmare Edition 663
Raj Gopalakrishna, Rajaram Bhaskaran

VelLMes: A High-Interaction AI-Based Deception Framework 672
Muris Sladić, Veronica Valeros, Carlos Catania, Sebastian Garcia

A Case Study on the Use of Representativeness Bias as a Defense Against Adversarial Cyber Threats 681
Briland Hitaj, Grit Denker, Laura Tinnel, Michael McAnally, Bruce DeBruhl, Nathan Bunting, Alex Fafard
Daniel Aaron, Richard D. Roberts, Joshua Lawson, Greg McCain, Dylan Starink

Koney: A Cyber Deception Orchestration Framework for Kubernetes 691
Mario Kahlhofer, Matteo Golinelli, Stefan Rass

Detection of Reverse Engineering Activities Before the Attack 704
Paolo Falcarin, Mirco Venerba, Matteo De Giorgi, Federica Sarro