2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2023)

Delft, Netherlands
3-7 July 2023

IEEE Catalog Number: CFP23N35-POD
ISBN: 979-8-3503-2721-2

Copyright © 2023 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:	CFP23N35-POD
ISBN (Print-On-Demand):	979-8-3503-2721-2
ISBN (Online):	979-8-3503-2720-5
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

CURRAN ASSOCIATES INC.
proceedings
.com

2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)

EuroSPW 2023

Table of Contents

Welcome Message from the General Chairs .... **xiv**
Welcome Message from the Workshop Chairs .... **xv**

ACSW: Automotive Cyber Security Workshop

A Threat Model for Soft Privacy on Smart Cars 1
Mario Raciti (Università degli Studi di Catania, Italy) and Giampaolo Bella (Università degli Studi di Catania, Italy)

Vulnerability Analysis of Vehicular Coordinated Maneuvers 11
Konstantinos Kalogiannis (KTH Royal Institute of Technology, Sweden), Andreas Henriksson (KTH Royal Institute of Technology, Sweden), and Panos Papadimitratos (KTH Royal Institute of Technology, Sweden)

DevSecOpsRO: Research and Opportunities on Secure Software Development

A Preliminary Study of Privilege Life Cycle in Software Management Platform Automation Workflows 21
Giacomo Benedetti (University of Genoa, Italy), Luca Verderame (University of Genoa, Italy), and Alessio Merlo (CASD - Centre for High Defense Studies, Italy)

An Investigation of Quality Issues in Vulnerability Detection Datasets 29
Yuejun Guo (Luxembourg Institute of Science and Technology, Luxembourg) and Seifeddine Bettaieb (Luxembourg Institute of Science and Technology, Luxembourg)

GLICE: Combining Graph Neural Networks and Program Slicing to Improve Software Vulnerability Detection 34
Wesley De Kraker (Open University in the Netherlands, The Netherlands), Harald Vranken (Open University in the Netherlands, The Netherlands), and Arjen Hommersom (Open University in the Netherlands, The Netherlands)

Guiding Directed Fuzzing with Feasibility 42
Weiheng Bai (University of Minnesota-Twin Cities, USA), Kefu Wu (University of Minnesota - Twin Cities, USA), Qiushi Wu (University of Minnesota - Twin Cities, USA), and Kangjie Lu (University of Minnesota - Twin Cities, USA)

Effective Machine Learning-based Access Control Administration through Unlearning 50
Javier Martínez Llamas (imec-DistriNet, KU Leuven, Belgium), Davy Preuveneers (imec-DistriNet, KU Leuven, Belgium), and Wouter Joosen (imec-DistriNet, KU Leuven, Belgium)

An Analysis System to Test Security of Software on Continuous Integration-Continuous Delivery Pipeline 58
Carmelo Aparo (Desys s.r.l., Italy), Cinzia Bernardeschi (University of Pisa, Italy), Giuseppe Lettieri (University of Pisa, Italy), Fabio Lucattini (Desys s.r.l., Italy), and Salvatore Montanarella (Desys s.r.l., Italy)

Tales from the Git: Automating the Detection of Secrets on Code and Assessing Developers' Passwords Choices 68
Nikolaos Lykoysas (Data Centric) and Constantinos Patsakis (University of Piraeus)

IWPE: International Workshop on Privacy Engineering

A ‘Human-in-the-Loop’ Approach for Information Extraction from Privacy Policies under Data Scarcity 76
Michael Gebauer (Information Systems Engineering - TU Berlin, Berlin), Faraz Maschhur (Information Systems Engineering - TU Berlin, Berlin), Nicola Leschke (Information Systems Engineering - TU Berlin, Berlin), Elias Grünewald (Information Systems Engineering - TU Berlin, Berlin), and Frank Pallas (Information Systems Engineering - TU Berlin, Berlin)

An Analysis of Requirements and Privacy Threats in Mobile Data Donations 84
Leonie Reichert (Humboldt University Berlin) and Björn Scheuermann (TU Darmstadt)

ATLAS: Automatically Detecting Discrepancies Between Privacy Policies and Privacy Labels 94
Akshath Jain (Carnegie Mellon University), David Rodriguez (Universidad Politécnica de Madrid), Jose M. del Alamo (Universidad Politécnica de Madrid), and Norman Sadeh (Carnegie Mellon University)

Automating Privacy Decisions – Where to Draw the Line? 108
Victor Morel (Chalmers University of Technology, Sweden) and Simone Fischer-Hübnerr (Chalmers University of Technology & Karlstad University, Sweden)

Lessons Learned: Building a Privacy-Preserving Entity Resolution Adaptation of PPJoin using End-to-End Homomorphic Encryption 117
Tanmay Ghai (Information Sciences Institute, USA), Yixiang Yao (University of Southern California, USA), and Srivatsan Ravi (University of Southern California, USA)

Privacy as an Architectural Quality: A Definition and an Architectural View 125
Immanuel Kunz (Fraunhofer AISEC, Germany) and Shuqian Xu (Technical University of Munich, Germany)

Secure Key Management for Multi-Party Computation in MOZAIK 133
Enzo Marquet (KU Leuven, Belgium), Jerico Moeyersons (Ghent University, Belgium), Erik Pohle (KU Leuven, Belgium), Michiel Van Kenhove (Ghent University, Belgium), Aysajan Abidin (KU Leuven, Belgium), and Bruno Volckaert (Ghent University, Belgium)

Unified Communication: What do Digital Activists Need? 141
Thomas Reisinger (De Montfort University, United Kingdom), Isabel Wagner (University of Basel, Switzerland), and Eerke Albert Boiten (De Montfort University, United Kingdom)

Comparing Privacy Label Disclosures of Apps Published in Both the App Store and Google Play Stores 150
David Rodriguez (Universidad Politécnica de Madrid), Akshath Jain (Carnegie Mellon University), Jose M. del Alamo (Universidad Politécnica de Madrid), and Norman Sadeh (Carnegie Mellon University)

WACCO: Workshop on Attackers and Cyber-Crime Operations

"Get a Higher Return on Your Savings!": Comparing Adverts for Cryptocurrency Investment Scams Across Platforms 158
Gilberto Atondo Siu (University of Cambridge, United Kingdom) and Alice Hutchings (University of Cambridge, United Kingdom)

An Argument for Linguistic Expertise in Cyberthreat Analysis: LOLSec in Russian Language eCrime Landscape 170
Dalyapraz Manatova (Indiana University), L Jean Camp (Indiana University, USA), Julia R. Fox (Indiana University, USA), Sandra Kuebler (Indiana University, USA), Maria A. Shardakova (Indiana University, USA), and Inna Kouper (Indiana University, USA)

Applying Neutralisation Theory to Better Understand Ransomware Offenders 177
Lena Connolly (Zayed University, UAE), Hervé Borrion (University College London, United Kingdom), Budi Arief (University of Kent, United Kingdom), and Sanaa Kaddoura (Zayed University, UAE)

Digital Drift and the Evolution of a Large Cybercrime Forum 183
Jack Hughes (University of Cambridge, UK) and Alice Hutchings (University of Cambridge, UK)

Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights 194
Jay Jacobs (Cyentia Institute), Sasha Romanosky (RAND Corporation), Octavian Suciu (University of Maryland), Ben Edwards (Cyentia Institute), and Armin Sarabi (University of Michigan)

How Cryptocurrency Exchange Interruptions Create Arbitrage Opportunities 207
Andrew Morin (The University of Tulsa, USA) and Tyler Moore (The University of Tulsa, USA)

Mapping the Cyberstalking Landscape: An Empirical Analysis of Federal U.S. Crimes 216
Sasha Romanosky (RAND, USA) and Peter Schirmer (RAND, USA)

On Gaps in Enterprise Cyber Attack Reporting 227
Abulfaz Hajizada (The University of Tulsa, USA) and Tyler Moore (The University of Tulsa, USA)

The Peculiar Case of Tailored Phishing against SMEs: Detection and Collective Defense Mechanisms at a Small IT Company 232
Pavlo Burda (Eindhoven University of Technology), Abdul Malek Altawekji (Eindhoven University of Technology), Luca Allodi (Eindhoven University of Technology), and Nicola Zannone (Eindhoven University of Technology)

Visualizing Cyber-Threats in Underground Forums 244
James Burroughs (King's College London, United Kingdom), Michal Tereszkowski-Kaminski (King's College London, United Kingdom), and Guillermo Suarez-Tangil (IMDEA Networks Institute, Spain)

SILM: Workshop on Security of Software/Hardware Interfaces

A Hybrid Solution for Constrained Devices to Detect Microarchitectural Attacks 259
Nikolaos-Foivos Polychronou (Univ. Grenoble Alpes, CEA, LETI, DSYS, LSES, France), Pierre-Henri Thevenon (Univ. Grenoble Alpes, CEA, LETI, DSYS, LSES, France), Maxime Puys (Univ. Grenoble Alpes, CEA, LETI, DSYS, LSES, France), and Vincent Beroulle (Univ. Grenoble Alpes, Grenoble-INP, LCIS, France)

A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards 270
Joshua Harrison (Durham University, UK), Ehsan Toreini (University of Surrey, UK), and Maryam Mehrnezhad (University of London, UK)

Combined Internal Attacks on SoC-FPGAs: Breaking AES with Remote Power Analysis and Frequency-based Covert Channels 281
Anis Fellah-Touta (UJM Saint-Etienne, CNRS, Institut d Optique Graduate School, France), Lilian Bossuet (UJM Saint-Etienne, CNRS, Institut d Optique Graduate School, France), and Carlos Andres Lara-nino (UJM Saint-Etienne, CNRS, Institut d Optique Graduate School, France)

Emulating Side Channel Attacks on Gem5: Lessons Learned 287
Lilian Bossuet (UJM Saint-Etienne, CNRS, France), Vincent Grosso (UJM Saint-Etienne, CNRS, France), and Carlos Andres Lara-Nino (UJM Saint-Etienne, CNRS, France)

TimeInspector: A Static Analysis Approach for Detecting Timing Attacks 296
Fatih Durmaz (Sabanci University, Turkey), Nureddin Kamadan (Sabanci University, Turkey), Melih Taha Öz (Sabanci University, Turkey), Musa Unal (Sabanci University, Turkey), Arsalan Javeed (Sabanci University, Turkey), Cemal Yilmaz (Sabanci University, Turkey), and Erkay Savas (Sabanci University, Turkey)

Work in Progress: Thwarting Timing Attacks in Microcontrollers using Fine-Grained Hardware Protections 304
Nicolas Gaudin (Univ. Bretagne-Sud, France), Jean-Loup Hatchikian-Houdot (Univ. Rennes, France), Frédéric Besson (Univ. Rennes, France), Pascal Cotret (UMR 6285, Lab-STICC, ENSTA Bretagne, France), Guy Gogniat (Univ. Bretagne-Sud, France), Guillaume Hiet (Univ. Rennes, France), Vianney Lapotre (Univ. Bretagne-Sud, France), and Pierre Wilke (Univ. Rennes, France)

Faulting Original McEliece's Implementations is Possible How to Mitigate this Risk? 311
Vincent Giraud (PSL University, France) and Guillaume Bouffard (PSL University, France)

RICSS: International Workshop on Re-design Industrial Control Systems with Security

A Digital Forensic Taxonomy For Programmable Logic Controller Data Artefacts 320
Feras Shahbi (University of Bristol, UK), Joseph Gardiner (University of Bristol, UK), Sridhar Adepu (University of Bristol, UK), and Awais Rashid (University of Bristol, UK)

A Key to Embedded System Security: Locking and Unlocking Secrets with a Trusted Platform Module 329
Teri Lenard (University of Geneva, Switzerland), Anastasija Collen (University of Geneva, Switzerland), Niels A. Nijdam (University of Geneva, Switzerland), and Bela Genge (University of Medicine, Romania)

From Tactics to Techniques: A Systematic Attack Modeling for Advanced Persistent Threats in Industrial Control Systems 336
Yunhe Yang (University of Utah, USA) and Mu Zhang (University of Utah, USA)

The Bandit's States: Modeling State Selection for Stateful Network Fuzzing as Multi-armed Bandit Problem 345
Anne Borcherding (Fraunhofer IOSB, Germany), Mark Giraud (Fraunhofer IOSB, Germany), Ian Fitzgerald (Karlsruhe Institute of Technology, Germany), and Jürgen Beyerer (Fraunhofer IOSB, Karlsruhe Institute of Technology, and KASTEL Security Research Labs, Germany)

The Case for Virtual PLC-Enabled Honeypot Design 351
Samin Y. Chowdhury (Florida International University), Brandon Dudley (Dragos, Inc.), and Ruimin Sun (Florida International University)

To me, to you: Towards Secure PLC Programming through a Community-Driven Open-Source Initiative 358
Richard Derbyshire (Orange Cyberdefense, United Kingdom), Sam Maesschalck (Lancaster University, United Kingdom), Alexander Staves (Lancaster University, United Kingdom), Benjamin Green (Lancaster University, United Kingdom), and David Hutchison (Lancaster University, United Kingdom)

Unsafe Behavior Detection with Adaptive Contrastive Learning in Industrial Control Systems....... 363
Xu Zheng (Florida International University, USA), Tianchun Wang (Pennsylvania State University, USA), Samin Yasar Chowdhury (Florida International University, USA), Ruimin Sun (Florida International University, USA), and Dongsheng Luo (Florida International University, USA)

ARCSG: Advancing Resilience of Cyber-Physical Smart Grid: An Integrated Co-Simulation Approach Incorporating Indicators of Compromise 370
Mohammed Asiri (Cardiff University, UK), Neetesh Saxena (Cardiff University, UK), and Pete Burnap (Cardiff University, UK)

Re-Envisioning Industrial Control Systems Security by Considering Human Factors as a Core Element of Defense-in-Depth 379
Jens Pottebaum (Paderborn University, Germany; Heinz Nixdorf Institute, Germany), Jost Rossel (Paderborn University, Germany), Juraj Somorovsky (Paderborn University, Germany), Yasemin Acar (Paderborn University, The George Washington University, USA), René Fahr (Paderborn University, Germany; Heinz Nixdorf Institute, Germany), Patricia Arias Cabarcos (Paderborn University, Germany), Eric Bodden (Paderborn University, Germany; Heinz Nixdorf Institute, Germany; Fraunhofer IEM, Germany), and Iris Gräßler (Paderborn University, Germany; Heinz Nixdorf Institute, Germany)

LPW: Location Privacy Workshop

D-GATE: Decentralized Geolocation and Time Enforcement for Usage Control 386
Hendrik Meyer Zum Felde (Fraunhofer AISEC, Germany), Jean-Luc Reding (Fraunhofer AISEC, Germany), and Michael Lux (Fraunhofer AISEC, Germany)

Hexanonymity: a Scalable Geo-Positioned Data Clustering Algorithm for Anonymisation Purposes 396
Javier Rodriguez-Viñas (GRADIANT, Spain), Ines Ortega-Fernandez (GRADIANT, Spain; Universidade de Vigo, Spain), and Eva Sotos Martínez (GRADIANT, Spain)

Masking Location Streams in the Presence of Colluding Service Providers 405
Toon Dehaene (KU Leuven, Belgium), Michiel Willocx (KU Leuven, Belgium), Bert Lagaisse (KU Leuven, Belgium), and Vincent Naessens (KU Leuven, Belgium)

WoRMA: Workshop on Robust Malware Analysis

A Wolf in Sheep's Clothing: Query-Free Evasion Attacks Against Machine Learning-Based Malware Detectors with Generative Adversarial Networks 415
Daniel Gibert (CeADAR/University College Dublin, Ireland), Jordi Planes (University of Lleida, Spain), Quan Le (CeADAR/University College Dublin, Ireland), and Giulio Zizzo (IBM Research Europe, Ireland)

Simplification of General Mixed Boolean-Arithmetic Expressions: GAMBA 427
Benjamin Reichenwallner (Denuvo GmbH, Austria) and Peter Meerwald-Stadler (Denuvo GmbH, Austria)

Temporal Analysis of Distribution Shifts in Malware Classification for Digital Forensics 439
Francesco Zola (Vicomtech, Basque Research and Technology Alliance (BRTA), Spain), Jan Lukas Bruse (Vicomtech, Basque Research and Technology Alliance (BRTA), Spain), and Mikel Galar (Public University of Navarre, Spain)

AD&D: Workshop on Active Defense and Deception

How Well does GPT Phish People? An Investigation Involving Cognitive Biases and Feedback 451
Megha Sharma (Indian Institute of Technology Mandi, India), Kuldeep Singh (University of Texas at El Paso, USA), Palvi Aggarwal (University of Texas at El Paso, USA), and Varun Dutt (Indian Institute of Technology Mandi, India)

Learning to Defend by Attacking (and Vice-Versa): Transfer of Learning in Cybersecurity Games 458
Tyler Malloy (Carnegie Mellon University) and Cleotilde Gonzalez (Carnegie Mellon University)

Honey Infiltrator: Injecting Honeytoken Using Netfilter 465
Daniel Reti (German Research Center for Artificial Intelligence GmbH (DFKI), Germany), Tillmann Angeli (German Research Center for Artificial Intelligence GmbH (DFKI), Germany), and Hans Dieter Schotten (German Research Center for Artificial Intelligence GmbH (DFKI), Germany; RPTU Kaiserslautern-Landau, Germany)

WTMC: International Workshop on Traffic Measurements for Cybersecurity

A First Look at SVCB and HTTPS DNS Resource Records in the Wild 470
Johannes Zirngibl (Technical University of Munich, Germany), Patrick Sattler (Technical University of Munich, Germany), and Georg Carle (Technical University of Munich, Germany)

Assessing and Exploiting Domain Name Misinformation 475
Blake Anderson (Cisco) and David McGrew (Cisco)

Assessing Network Operator Actions to Enhance Digital Sovereignty and Strengthen Network Resilience: A Longitudinal Analysis during the Russia-Ukraine Conflict 487
Muhammad Yasir Muzayan Haq (University of Twente, The Netherlands), Abhishta Abhishta (University of Twente, The Netherlands), Raffaele Sommese (University of Twente, The Netherlands), Mattijs Jonker (University of Twente, The Netherlands), and Lambert J.M. Nieuwenhuis (University of Twente, The Netherlands)

Detecting and Analyzing Mouse Tracking in the Wild 495
Marcel Urpí-Bricollé (Universitat Politècnica de Catalunya, Spain), Ismael Castell-Uroz (Universitat Politècnica de Catalunya, Spain), and Pere Barlet-Ros (Universitat Politècnica de Catalunya, Spain)

Inside Residential IP Proxies: Lessons Learned from Large Measurement Campaigns 501
Elisa Chiapponi (EURECOM, France), Marc Dacier (RC3, CEMSE, KAUST, Kindom of Saudi Arabia), and Olivier Thonnard (Amadeus IT Group, France)

Lost in Translation: AI-based Generator of Cross-Language Sound-Squatting 513
Rodolfo Valentim (Politecnico di Torino), Idilio Drago (Università di Torino), Marco Mellia (Politecnico di Torino), and Federico Cerutti (Università degli Studi di Brescia)

Revisiting OAuth 2.0 Compliance: A Two-Year Follow-Up Study 521
Pieter Philippaerts (imec-DistriNet, KU Leuven, Belgium), Davy Preuveneers (imec-DistriNet, KU Leuven, Belgium), and Wouter Joosen (imec-DistriNet, KU Leuven, Belgium)

TLS Post-Quantum TLS: Inspecting the TLS Landscape for PQC Adoption on Android 526
Dimitri Mankowski (Ruhr University Bochum, Germany), Thom Wiggers (PQShield, The Netherlands), and Veelasha Moonsamy (Ruhr University Bochum, Germany)

Towards More Rigorous Domain-based Metrics: Quantifying the Prevalence and Implications of "Active" Domains 539
Siôn Lloyd (ICANN), Carlos Hernandez-Gañan (ICANN), and Samaneh Tajalizadehkhoob (ICANN)

Unveiling the Weak Links: Exploring DNS Infrastructure Vulnerabilities and Fortifying Defenses 546
Yevheniya Nosyk (Université Grenoble Alpes, France), Olivier Hureau (Université Grenoble Alpes, France), Simon Fernandez (Université Grenoble Alpes, France), Andrzej Duda (Université Grenoble Alpes, France), and Maciej Korczyński (Université Grenoble Alpes, France)

Fake it Till You Detect it: Continual Anomaly Detection in Multivariate Time-Series using Generative AI 558
Gastón García González (Universidad de la República, Uruguay), Pedro Casas (Austrian Institute of Technology, Austria), and Alicia Fernández (Universidad de la República, Uruguay)

Identifying and Differentiating Acknowledged Scanners in Network Traffic 567
M. Patrick Collins (USC Information Sciences Institute, USA), Alefiya Hussian (USC Information Sciences Institute, USA), and Stephen Schwab (USC Information Sciences Institute, USA)

STAST: Workshop on Socio-Technical Aspects in Security

”As Usual, I Needed Assistance of a Seeing Person”: Experiences and Challenges of People with Disabilities and Authentication Methods 575
Erinola Ahmet (Materna Information & Communications SE, Germany), Annalina Buckmann (Ruhr University Bochum, Germany), Jennifer Friedauer (Ruhr University Bochum, Germany), Asli Yardim (Ruhr University Bochum, Germany), and M. Angela Sasse (Ruhr University Bochum, Germany)

Talking Abortion (Mis)information with ChatGPT on TikTok 594
Filipo Sharevski (DePaul University, USA), Jennifer Vander Loop (DePaul University, USA), Peter Jachim (DePaul University, USA), Amy Devine (DePaul University, USA), and Emma Pieroni (DePaul University, USA)

Work in Progress: A Glance at Social Media Self-Censorship in North America 609
Wei Hu (University of Waterloo, Canada) and Diogo Barradas (University of Waterloo, Canada)

Position Paper: The Role of law in Achieving Privacy and Security Measures in Smart Buildings from the GDPR Context 619
Natalie Leesakul (Newcastle University, United Kingdom) and Charles Morisset (Newcastle University, United Kingdom)

Divided We Hack: Exploring the Degree of Sino-Russian Coordination in Cyberspace During the Ukraine War 627
Francesco Ferazza (University of London, United Kingdom), Cosimo Melella (University of Genoa, Italy), Konstantinos Mersinas (University of London, United Kingdom), and Antonio Calcara (University of Antwerp, Belgium)

U-Sense: Feasibility Study of "Human as a Sensor" in Incident Reporting Systems in a Smart Campus 641
Naoom Abu Abah (Newcastle University, UK), Nick Taylor (Newcastle University, UK), Charles Morisset (Newcastle University, UK), and Maryam Mehrnezhad (University of London, UK)

Work in Progress: Evaluation of Security Standards through a Cyber Range using Hackers' Tactics, Techniques and Procedures 653
Patrick Wake (Durham University, UK), Sue Black (Durham University, UK), and Jonathan Young (Durham University, UK)

What We Do in the Shadows: How does Experiencing Cybercrime Affect Response Actions & Protective Practices? 659
Magdalene Ng (University of Westminster, UK), Maria Bada (Queen Mary University of London, UK), and Kovila P.L. Coopamootoo (King's College London, UK)

Author Index **673**