2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P 2023)

Delft, Netherlands
3-7 July 2023

Pages 1-630

IEEE Catalog Number: CFP23C75-POD
ISBN: 978-1-6654-6513-7

1/2

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:	CFP23C75-POD
ISBN (Print-On-Demand):	978-1-6654-6513-7
ISBN (Online):	978-1-6654-6512-0

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 8th European Symposium on Security and Privacy (EuroS&P)

EuroSP 2023

Table of Contents

Welcome Message from the General Chairs ... **xiv**
Welcome Message from the PC Chairs ... **xv**
Euro S&P 2023 Steering Committee ... **xvi**
Euro S&P 2023 Organizing Committee ... **xvii**
Euro S&P 2023 Program Committee ... **xviii**

Phishing/fraud/scams

Android, Notify Me When it is Time to Go Phishing ... 1
Antonio Ruggia (University of Genoa, Italy), Andrea Possemato (EURECOM, France), Alessio Merlo (Centre for Higher Defence Studies (CASD), Italy), Dario Nisi (EURECOM, France), and Simone Aonzo (EURECOM, France)

Understanding, Measuring, and Detecting Modern Technical Support Scams ... 18
Jienan Liu (University of Georgia), Pooja Pun (University of New Orleans), Phani Vadrevu (University of New Orleans), and Roberto Perdisci (University of Georgia; Georgia Institute of Technology)

Active Countermeasures for Email Fraud ... 39
Wentao Chen (University of Bristol, United Kingdom), Fuzhou Wang (City University of Hong Kong, Hong Kong SAR), and Matthew Edwards (University of Bristol, United Kingdom)

Crypto + formal methods I

Multi-factor Credential Hashing for Asymmetric Brute-Force Attack Resistance ... 56
Vivek Nair (UC Berkeley) and Dawn Song (UC Berkeley)

CHEX-MIX: Combining Homomorphic Encryption with Trusted Execution Environments for Oblivious Inference in the Cloud ... 73
Deepika Natarajan (University of Michigan), Andrew Loveless (University of Michigan), Wei Dai (Microsoft Research), and Ron Dreslinski (University of Michigan)

A Generic Obfuscation Framework for Preventing ML-Attacks on Strong-PUFs through Exploitation of DRAM-PUFs 92
Owen Millwood (The University of Sheffield, UK), Meltem Kurt Pehlivanoğlu (Kocaeli University, Turkey), Aryan Mohammadi Pasikhani (University of Sheffield, UK), Jack Miskelly (Queen's University Belfast, United Kingdom), Prosanta Gope (University of Sheffield, UK), and Elif Bilge Kavun (University of Passau, Germany)

Automatic Verification of Transparency Protocols 107
Vincent Cheval (Inria Paris, France), José Moreira (Valory AG, Switzerland), and Mark Ryan (University of Birmingham, United Kingdom)

SoK: Data Sovereignty 122
Jens Ernstberger (Technical University of Munich, Germany; Berkeley Center for Responsible, Decentralized Intelligence (RDI)), Jan Lauinger (Technical University of Munich, Germany), Fatima Elsheimy (Yale University, USA), Liyi Zhou (Imperial College London, United Kingdom; Berkeley Center for Responsible, Decentralized Intelligence (RDI)), Sebastian Steinhorst (Technical University of Munich, Germany), Ran Canetti (Boston University, USA), Andrew Miller (University of Illinois at Urbana-Champaign, USA), Arthur Gervais (University College London, United Kingdom; Berkeley Center for Responsible, Decentralized Intelligence (RDI)), and Dawn Song (University of California, Berkeley, USA; Berkeley Center for Responsible, Decentralized Intelligence (RDI))

Security and AI

An Unbiased Transformer Source Code Learning with Semantic Vulnerability Graph 144
Nafis Tanveer Islam (University of Texas at San Antonio), Gonzalo De La Torre Parra (University of the Incarnate Word), Dylan Manuel (University of Texas at San Antonio), Elias Bou-Harb (University of Texas at San Antonio), and Peyman Najafirad (University of Texas at San Antonio)

Protecting Voice-Controllable Devices Against Self-Issued Voice Commands 160
Sergio Esposito (University of London, United Kingdom), Daniele Sgandurra (University of London, United Kingdom), and Giampaolo Bella (Università degli Studi di Catania, Italy)

When the Curious Abandon Honesty: Federated Learning Is Not Private 175
Franziska Boenisch (Vector Institute), Adam Dziedzic (Vector Institute; University of Toronto), Roei Schuster (Vector Institute), Ali Shahin Shamsabadi (Vector Institute; The Alan Turing Institute), Ilia Shumailov (Vector Institute), and Nicolas Papernot (Vector Institute; University of Toronto)

A Certified Radius-Guided Attack Framework to Image Segmentation Models 200
Wenjie Qu (Huazhong University of Science and Technology, China), Youqi Li (School of Computer Sci. & Tech., Beijing Institute of Technology, China), and Binghui Wang (Illinois Institute of Technology, USA)

SoK: Explainable Machine Learning for Computer Security Applications 221
Azqa Nadeem (Delft University of Technology, The Netherlands), Daniël Vos (Delft University of Technology, The Netherlands), Clinton Cao (Delft University of Technology, The Netherlands), Luca Pajola (University of Padua, Italy), Simon Dieck (Delft University of Technology, The Netherlands), Robert Baumgartner (Delft University of Technology, The Netherlands), and Sicco Verwer (Delft University of Technology, The Netherlands)

Privacy

Reconstructing Individual Data Points in Federated Learning Hardened with Differential Privacy and Secure Aggregation 241
Franziska Boenisch (Vector Institute), Adam Dziedzic (Vector Institute; University of Toronto), Roei Schuster (Vector Institute), Ali Shahin Shamsabadi (Vector Institute; The Alan Turing Institute), Ilia Shumailov (Vector Institute), and Nicolas Papernot (Vector Institute; University of Toronto)

Towards Fine-Grained Localization of Privacy Behaviors 258
Vijayanta Jain (University of Maine), Sepideh Ghanavati (University of Maine), Sai Teja Peddinti (Google Inc.), and Collin McMillan (University of Notre Dame)

Masterkey Attacks Against Free-Text Keystroke Dynamics and Security Implications of Demographic Factors 278
Tim Van Hamme (imec - DistriNet, KU Leuven, Belgium), Giuseppe Garofalo (imec - DistriNet, KU Leuven, Belgium), Davy Preuveneers (imec - DistriNet, KU Leuven, Belgium), and Wouter Joosen (imec - DistriNet, KU Leuven, Belgium)

"Act Natural!": Exchanging Private Messages on Public Blockchains 292
Thore Tiemann (University of Lübeck, Germany), Sebastian Berndt (University of Lübeck, Germany), Thomas Eisenbarth (University of Lübeck, Germany), and Maciej Liśkiewicz (University of Lübeck, Germany)

smartFHE: Privacy-Preserving Smart Contracts from Fully Homomorphic Encryption 309
Ravital Solomon (Sunscreen, USA), Rick Weber (Sunscreen, USA), and Ghada Almashaqbeh (University of Connecticut, USA)

Online Videos

Understanding the Security Risks of Decentralized Exchanges by Uncovering Unfair Trades in the Wild 332
Jiaqi Chen (Syracuse University), Yibo Wang (Syracuse University), Yuxuan Zhou (Syracuse University), Wanning Ding (Syracuse University), Yuzhe Tang (Syracuse University), XiaoFeng Wang (Indiana University Bloomington), and Kai Li (San Diego State University; Syracuse University)

MISO: Legacy-Compatible Privacy-Preserving Single Sign-on using Trusted Execution Environments ... 352
Rongwu Xu (Tsinghua University), Sen Yang (Yale University), Fan Zhang (Yale University, USA), and Zhixuan Fang (Tsinghua University, China; Shanghai Qi Zhi Institute)

Forward Pass: On the Security Implications of Email Forwarding Mechanism and Policy ... 373
Enze Liu (UC San Diego, USA), Gautam Akiwate (Stanford University, USA), Mattijs Jonker (University of Twente, USA), Ariana Mirian (UC San Diego, USA), Grant Ho (UC San Diego, USA), Geoffrey M. Voelker (UC San Diego, USA), and Stefan Savage (UC San Diego, USA)

Privformer: Privacy-Preserving Transformer with MPC ... 392
Yoshimasa Akimoto (University of Tsukuba, Japan), Kazuto Fukuchi (University of Tsukuba, Japan), Youhei Akimoto (University of Tsukuba, Japan), and Jun Sakuma (Tokyo Institute of Technology, Japan)

Coverage and Secure Use Analysis of Content Security Policies via Clustering ... 411
Mengxia Ren (Colorado School of Mines, USA) and Chuan Yue (Colorado School of Mines, USA)

CommiTEE: An Efficient and Secure Commit-Chain Protocol using TEEs ... 429
Andreas Erwig (TU Darmstadt, Germany), Sebastian Faust (TU Darmstadt, Germany), Siavash Riahi (TU Darmstadt, Germany), and Tobias Stöckert (Fraunhofer SIT, Germany)

Fuzzing & Vulnerability finding

EF\CF: High Performance Smart Contract Fuzzing for Exploit Generation ... 449
Michael Rodler (University of Duisburg-Essen; Amazon Web Services), David Paaßen (University of Duisburg-Essen), Wenting Li (NEC Laboratories Europe), Lukas Bernhard (Ruhr-University Bochum), Thorsten Holz (CISPA Helmholtz Center for Information Security), Ghassan Karame (Ruhr-University Bochum), and Lucas Davi (University of Duisburg-Essen)

Fuzzing SGX Enclaves via Host Program Mutations ... 472
Arslan Khan (Purdue University), Muqi Zou (Purdue University), Kyungtae Kim (Purdue University), Dongyan Xu (Purdue University), Antonio Bianchi (Purdue University), and Dave Jing Tian (Purdue University)

Finding Fixed Vulnerabilities with Off-the-Shelf Static Analysis ... 489
Trevor Dunlap (North Carolina State University, USA), Seaver Thorn (North Carolina State University, USA), William Enck (North Carolina State University, USA), and Bradley Reaves (North Carolina State University, USA)

Code Vulnerability Detection via Signal-Aware Learning ... 506
Sahil Suneja (IBM Research, USA), Yufan Zhang (University of California San Diego, USA), Yunhui Zheng (IBM Research, USA), Jim Laredo (IBM Research, USA), Alessandro Morari (IBM Research, USA), and Udayan Khurana (IBM Research, USA)

Hunting for Truth: Analyzing Explanation Methods in Learning-based Vulnerability Discovery.... 524
Tom Ganz (SAP SE, Germany), Philipp Rall (Technische Universität Darmstadt, Germany), Martin Härterich (SAP SE, Germany), and Konrad Rieck (Technische Universität Berlin, Germany)

Networks

Systematic Improvement of Access-Stratum Security in Mobile Networks 542
Rhys Miller (University of Surrey, UK), Ioana Boureanu (University of Surrey, UK), Stephan Wesemeyer (University of Surrey, UK), Zhili Sun (University of Surrey, UK), and Hemant Zope (Fraunhofer FOKUS, Germany)

Anomaly-based Filtering of Application-Layer DDoS Against DNS Authoritatives 558
Jonas Bushart (CISPA Helmholtz Center for Information Security, Germany) and Christian Rossow (CISPA Helmholtz Center for Information Security, Germany)

SoK: A Data-Driven View on Methods to Detect Reflective Amplification DDoS Attacks Using Honeypots 576
Marcin Nawrocki (Freie Universität Berlin), John Kristoff (University of Illinois at Chicago; NETSCOUT), Raphael Hiesgen (HAW Hamburg), Chris Kanich (University of Illinois at Chicago), Thomas C. Schmidt (HAW Hamburg), and Matthias Wählisch (TU Dresden; Freie Universität Berlin)

SoK: Pragmatic Assessment of Machine Learning for Network Intrusion Detection 592
Giovanni Apruzzese (Liechtenstein Business School – University of Liechtenstein), Pavel Laskov (Liechtenstein Business School – University of Liechtenstein), and Johannes Schneider (Liechtenstein Business School – University of Liechtenstein)

GNN4IFA: Interest Flooding Attack Detection with Graph Neural Networks 615
Andrea Agiollo (University of Bologna), Enkeleda Bardhi (Sapienza University of Rome), Mauro Conti (University of Padua; Delft University of Technology), Riccardo Lazzeretti (Sapienza University of Rome), Eleonora Losiouk (University of Padua), and Andrea Omicini (University of Bologna)

Side Channels and Transient Execution

SoK: Analysis of Root Causes and Defense Strategies for Attacks on Microarchitectural Optimizations 631
Nadja Ramhöj Holtryd (Chalmers University of Technology, Sweden), Madhavan Manivannan (Chalmers University of Technology, Sweden), and Per Stenström (Chalmers University of Technology, Sweden)

MicroProfiler: Principled Side-Channel Mitigation through Microarchitectural Profiling 651
Marton Bognar (imec-DistriNet, KU Leuven, Belgium), Hans Winderix (imec-DistriNet, KU Leuven, Belgium), Jo Van Bulck (imec-DistriNet, KU Leuven, Belgium), and Frank Piessens (imec-DistriNet, KU Leuven, Belgium)

You Cannot Always Win the Race: Analyzing Mitigations for Branch Target Prediction Attacks..... 671
Alyssa Milburn (Intel), Ke Sun (Intel), and Henrique Kawakami (Intel)

Towards Automated Detection of Single-Trace Side-Channel Vulnerabilities in Constant-Time Cryptographic Code 687
Ferhat Erata (Yale University), Ruzica Piskac (Yale University), Victor Mateu (Technology Innovation Institute), and Jakub Szefer (Yale University)

From Dragondoom to Dragonstar: Side-Channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake 707
Daniel De Almeida Braga (Univ Rennes, CNRS, IRISA), Natalia Kulatova (Mozilla), Mohamed Sabt (Univ Rennes, CNRS, IRISA), Pierre-Alain Fouque (Univ Rennes, CNRS, IRISA), and Karthikeyan Bhargavan (INIRIA Paris)

Crypto + formal methods II

Recurring Contingent Service Payment 724
Aydin Abadi (University College London, UK), Steven J. Murdoch (University College London, UK), and Thomas Zacharias (University College London, UK)

SIM: Secure Interval Membership Testing and Applications to Secure Comparison 757
Albert Yu (Purdue University), Donghang Lu (TikTok; Purdue University), Aniket Kate (Purdue University, Supra Research), and Hemanta K. Maji (Purdue University)

Careful with MAc-then-SIGn: A Computational Analysis of the EDHOC Lightweight Authenticated Key Exchange Protocol 773
Felix Günther (ETH Zurich, Switzerland) and Marc Ilunga Tshibumbu Mukendi (Trail of Bits, USA)

Proof-of-Learning is Currently More Broken Than You Think 797
Congyu Fang (University of Toronto; Vector Institute), Hengrui Jia (University of Toronto; Vector Institute), Anvith Thudi (University of Toronto; Vector Institute), Mohammad Yaghini (University of Toronto; Vector Institute), Christopher A. Choquette-Choo (Google Research (Brain Team)), Natalie Dullerud (University of Toronto; Vector Institute), Varun Chandrasekaran (Microsoft Research), and Nicolas Papernot (University of Toronto; Vector Institute)

Certifiably Vulnerable: Using Certificate Transparency Logs for Target Reconnaissance 817
Stijn Pletinckx (University of California, USA), Thanh-Dat Nguyen (Delft University of Technology, the Netherlands), Tobias Fiebig (Max Planck Institute for Informatics, Germany), Christopher Kruegel (University of California, USA), and Giovanni Vigna (University of California, USA)

Web and social media

Chrowned by an Extension: Abusing the Chrome DevTools Protocol through the Debugger API ... 832
José Miguel Moreno (Universidad Carlos III de Madrid, Spain), Narseo Vallina-Rodriguez (IMDEA Networks Institute, Spain), and Juan Tapiador (Universidad Carlos III de Madrid, Spain)

DarkDialogs: Automated Detection of 10 Dark Patterns on Cookie Dialogs 847
Daniel Kirkman (University of Edinburgh, UK), Kami Vaniea (University of Edinburgh, UK), and Daniel W Woods (University of Edinburgh, UK)

SoK: Content Moderation in Social Media, from Guidelines to Enforcement, and Research to Practice 868
Mohit Singhal (The University of Texas at Arlington), Chen Ling (Boston University), Pujan Paudel (Boston University), Poojitha Thota (The University of Texas at Arlington), Nihal Kumarswamy (The University of Texas at Arlington), Gianluca Stringhini (Boston University), and Shirin Nilizadeh (The University of Texas at Arlington)

SMART Credentials in the Multi-Queue of Slackness 896
Jack P. K. Ma (The Chinese University of Hong Kong, Hong Kong) and Sherman S. M. Chow (The Chinese University of Hong Kong, Hong Kong)

Been Here Already? Detecting Synchronized Browsers in the Wild 913
Pantelina Ioannou (University of Cyprus, Cyprus) and Elias Athanasopoulos (University of Cyprus, Cyprus)

Crypto + formal methods III

Asynchronous Remote Key Generation for Post-Quantum Cryptosystems from Lattices 928
Nick Frymann (University of Surrey, United Kingdom), Daniel Gardham (University of Surrey, United Kingdom), and Mark Manulis (Universität der Bundeswehr München, Germany)

Revelio: A Network-Level Privacy Attack in the Lightning Network 942
Theo von Arx (ETH Zürich), Muoi Tran (ETH Zurich), and Laurent Vanbever (ETH Zurich)

Conjunctive Searchable Symmetric Encryption from Hard Lattices 958
Debadrita Talapatra (IIT Kharagpur, India), Sikhar Patranabis (IBM Research, India), and Debdeep Mukhopadhyay (IIT Kharagpur, India)

Provable Adversarial Safety in Cyber-Physical Systems 979
John H. Castellanos (CISPA Helmholtz Center for Information Security, Germany), Mohamed Maghenem (University of Grenoble Alpes, CNRS, France), Alvaro A. Cárdenas (University of California, USA), Ricardo G. Sanfelice (University of California, USA), and Jianying Zhou (Singapore University of Technology and Design, Singapore)

Privately Evaluating Region Overlaps with Applications to Collaborative Sensor Output Validation 1013
Anrin Chakraborti (Duke University) and Michael K. Reiter (Duke University)

Analyzing attacks on things

Exploring Smart Commercial Building Occupants' Perceptions and Notification Preferences of Internet of Things Data Collection in the United States 1030
Tu Le (University of Virginia; University of California, Los Angeles), Alan Wang (University of Virginia), Yaxing Yao (University of Maryland, Baltimore County), Yuanyuan Feng (University of Vermont), Arsalan Heydarian (University of Virginia), Norman Sadeh (Carnegie Mellon University), and Yuan Tian (University of Virginia; University of California, Los Angeles)

AoT - Attack on Things: A Security Analysis of IoT Firmware Updates 1047
Muhammad Ibrahim (Purdue University, USA), Andrea Continella (University of Twente, Netherlands), and Antonio Bianchi (Purdue University, USA)

Comprehensively Analyzing the Impact of Cyberattacks on Power Grids 1065
Lennart Bader (Fraunhofer FKIE & RWTH Aachen University), Martin Serror (Fraunhofer FKIE), Olav Lamberts (Fraunhofer FKIE & RWTH Aachen University), Ömer Sen (Fraunhofer FIT & RWTH Aachen University), Dennis van der Velde (Fraunhofer FIT), Immanuel Hacker (Fraunhofer FIT & RWTH Aachen University), Julian Filter (RWTH Aachen University), Elmar Padilla (Fraunhofer FKIE), and Martin Henze (RWTH Aachen University & Fraunhofer FKIE)

SoK: Rethinking Sensor Spoofing Attacks against Robotic Vehicles from a Systematic View 1082
Yuan Xu (Nanyang Technological University), Xingshuo Han (Nanyang Technological University), Gelei Deng (Nanyang Technological University), Jiwei Li (Shannon.AI; Zhejiang University), Yang Liu (Nanyang Technological University), and Tianwei Zhang (Nanyang Technological University)

NodeMedic: End-to-End Analysis of Node.js Vulnerabilities with Provenance Graphs 1101
Darion Cassel (Carnegie Mellon University, USA), Wai Tuck Wong (Singapore Management University, Singapore), and Limin Jia (Carnegie Mellon University, USA)

Trusted computing and defenses

faulTPM: Exposing AMD fTPMs' Deepest Secrets 1128
Hans Niklas Jacob (Technische Universität Berlin, Berlin), Christian Werling (Technische Universität Berlin, Berlin), Robert Buhren (Technische Universität Berlin, Berlin), and Jean-Pierre Seifert (Fraunhofer SIT)

CHERI-TrEE: Flexible Enclaves on Capability Machines 1143
Thomas Van Strydonck (KU Leuven), Job Noorman (KU Leuven), Jennifer Jackson (University of Birmingham), Leonardo Alves Dias (University of Birmingham), Robin Vanderstraeten (Vrije Universiteit Brussel), David Oswald (University of Birmingham), Frank Piessens (KU Leuven), and Dominique Devriese (KU Leuven)

SOK: Side Channel Monitoring for Additive Manufacturing - Bridging Cybersecurity and Quality Assurance Communities 1160
Muhammad Ahsan (Virginia Commonwealth University, USA), Muhammad Haris Rais (Virginia Commonwealth University, USA), and Irfan Ahmed (Virginia Commonwealth University, USA)

Watermarking Graph Neural Networks based on Backdoor Attacks 1179
Jing Xu (Delft University of Technology, Netherlands), Stefanos Koffas (Delft University of Technology, Netherlands), Oğuzhan Ersoy (Radboud University, Netherlands), and Stjepan Picek (Radboud University, Netherlands)

Author Index