# 2023 IEEE Symposium on Security and Privacy (SP 2023)

**San Francisco, California, USA**
**22-25 May 2023**

**Pages 1-754**

IEEE Catalog Number: CFP23020-POD
ISBN: 978-1-6654-9337-6

**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: | CFP23020-POD |
| ISBN (Print-On-Demand): | 978-1-6654-9337-6 |
| ISBN (Online): | 978-1-6654-9336-9 |
| ISSN: | 1081-6011 |

**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

# 2023 IEEE Symposium on Security and Privacy (SP)

# SP 2023

## Table of Contents

**Message from the General Chair** ........ xxxi
**Message from the Program Chairs** ........ xxxiv
**Organizing Committee** ........ xxxvi

## Session 1A: Infrastructure security

Space Odyssey: An Experimental Software Security Analysis of Satellites ........ N/A
*Johannes Willbold (Ruhr University Bochum), Moritz Schloegel (Ruhr University Bochum), Manuel Vögele (Ruhr University Bochum), Maximilian Gerhardt (Ruhr University Bochum), Thorsten Holz (CISPA Helmholtz Center for Information Security), and Ali Abbasi (CISPA Helmholtz Center for Information Security)*

SCAPHY: Detecting Modern ICS Attacks by Correlating Behaviors in SCADA and PHYsical ........ 20
*Moses Ike (Georgia Institute of Technology, USA), Kandy Phan (Sandia National Labs, USA), Keaton Sadoski (Sandia National Labs, USA), Romuald Valme (Sandia National Labs, USA), and Wenke Lee (Georgia Institute of Technology, USA)*

Shedding Light on Inconsistencies in Grid Cybersecurity: Disconnects and Recommendations ........ 38
*Brian Singer (Carnegie Mellon University), Amritanshu Pandey (Carnegie Mellon University), Shimiao Li (Carnegie Mellon University), Lujo Bauer (Carnegie Mellon University), Craig Miller (Carnegie Mellon University), Lawrence Pileggi (Carnegie Mellon University), and Vyas Sekar (Carnegie Mellon University)*

Red Team vs. Blue Team: A Real-World Hardware Trojan Detection Case Study Across Four Modern CMOS Technology Generations ........ 56
*Endres Puschner (Max Planck Institute for Security and Privacy, Germany), Thorben Moos (Université catholique de Louvain, Belgium), Steffen Becker (Ruhr University Bochum, Germany & Max Planck Institute for Security and Privacy, Germany), Christian Kison (Bundeskriminalamt, Germany), Amir Moradi (Ruhr University Bochum, Germany), and Christof Paar (Max Planck Institute for Security and Privacy, Germany)*

## Session 1B: Blockchain 1

SoK: Distributed Randomness Beacons ..... 75
*Kevin Choi (New York University, USA), Aathira Manoj (New York University, USA), and Joseph Bonneau (New York University, USA and a16z crypto research, USA)*

WeRLman: To Tackle Whale (Transactions), Go Deep (RL) ..... 93
*Roi Bar-Zur (Technion, IC3), Ameer Abu-Hanna (Technion), Ittay Eyal (Technion, IC3), and Aviv Tamar (Technion)*

Three Birds with One Stone: Efficient Partitioning Attacks on Interdependent Cryptocurrency Networks ..... 111
*Muhammad Saad (PayPal) and David Mohaisen (University of Central Florida)*

Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities ..... 126
*Ertem Nusret Tas (Stanford University), David Tse (Stanford University), Fangyu Gai (BabylonChain Inc.), Sreeram Kannan (University of Washington, Seattle), Mohammad Ali Maddah-Ali (University of Minnesota), and Fisher Yu (BabylonChain Inc.)*

## Session 1C: Cryptographic attacks

MEGA: Malleable Encryption Goes Awry ..... 146
*Matilda Backendal (ETH Zurich), Haller Miro (ETH Zurich), and Kenneth G. Paterson (ETH Zurich)*

Practically-exploitable Cryptographic Vulnerabilities in Matrix ..... N/A
*Martin R. Albrecht (King's College London), Sofía Celi (Brave Software), Benjamin Dowling (Security of Advanced Systems Group, University of Sheffield), and Daniel Jones (Information Security Group, Royal Holloway, University of London)*

DBREACH: Stealing from Databases Using Compression Side-Channels ..... 182
*Mathew Hogan (Stanford University), Yan Michalevsky (Anjuna Security, Inc and Cryptosat, Inc.), and Saba Eskandarian (UNC Chapel Hill)*

Weak Fiat-Shamir Attacks on Modern Proof Systems ..... 199
*Quang Dao (Carnegie Mellon University), Jim Miller (Trail of Bits), Opal Wright (Trail of Bits), and Paul Grubbs (University of Michigan)*

## Session 2A: Trust and safety

Attitudes towards Client-Side Scanning for CSAM, Terrorism, Drug Trafficking, Drug Use and Tax Evasion in Germany ..... 217
*Lisa Geierhaas (University of Bonn), Fabian Otto (OmniQuest), Maximilian Häring (University of Bonn), and Matthew Smith (University of Bonn, Fraunhofer FKIE)*

Deep perceptual hashing algorithms with hidden dual purpose: when client-side scanning does facial recognition ........ 234
*Shubham Jain (Imperial College London, United Kingdom), Ana-Maria Cretu (Imperial College London, United Kingdom), Antoine Cully (Imperial College London, United Kingdom), and Yves-Alexandre de Montjoye (Imperial College London, United Kingdom)*

Public Verification for Private Hash Matching ........ 253
*Sarah Scheffler (Princeton University), Anunay Kulshrestha (Princeton University), and Jonathan Mayer (Princeton University)*

Is Cryptographic Deniability Sufficient? Non-Expert Perceptions of Deniability in Secure Messaging ........ 274
*Nathan Reitinger (University of Maryland, USA), Nathan Malkin (University of Maryland, USA), Omer Akgul (University of Maryland, USA), Michelle L. Mazurek (University of Maryland, USA), and Ian Miers (University of Maryland, USA)*

On the Evolution of (Hateful) Memes by Means of Multimodal Contrastive Learning ........ 293
*Yiting Qu (CISPA Helmholtz Center for Information Security, Germany), Xinlei He (CISPA Helmholtz Center for Information Security, Germany), Shannon Pierson (London School of Economics and Political Science, UK), Michael Backes (CISPA Helmholtz Center for Information Security, Germany), Yang Zhang (CISPA Helmholtz Center for Information Security, Germany), and Savvas Zannettou (Delft University of Technology, Netherlands)*

LAMBRETTA: Learning to Rank for Twitter Soft Moderation ........ 311
*Pujan Paudel (Boston University), Jeremy Blackburn (Binghamton University), Emiliano De Cristofaro (University College London), Savvas Zannettou (Delft University of Technology), and Gianluca Stringhini (Boston University)*

## Session 2B: Machine learning privacy

SoK: Let the Privacy Games Begin! A Unified Treatment of Data Inference Privacy in Machine Learning ........ 327
*Ahmed Salem (Microsoft, United Kingdom), Giovanni Cherubin (Microsoft, United Kingdom), David Evans (University of Virginia, United States), Boris Koepf (Microsoft, United Kingdom), Andrew Paverd (Microsoft, United Kingdom), Anshuman Suri (University of Virginia, United States), Shruti Tople (Microsoft, United Kingdom), and Santiago Zanella-Beguelin (Microsoft, United Kingdom)*

Analyzing Leakage of Personally Identifiable Information in Language Models ........ 346
*Nils Lukas (University of Waterloo), Ahmed Salem (Microsoft Research), Robert Sim (Microsoft Research), Shruti Tople (Microsoft Research), Lukas Wutschitz (Microsoft Research), and Santiago Zanella-Béguelin (Microsoft Research)*

Accuracy-Privacy Trade-off in Deep Ensemble: A Membership Inference Perspective ........ 364
*Shahbaz Rezaei (University of California at Davis), Zubair Shafiq (University of California at Davis), and Xin Liu (University of California at Davis)*

D-DAE: Defense-Penetrating Model Extraction Attacks ........ 382
*Yanjiao Chen (Zhejiang University), Rui Guan (Wuhan University), Xueluan Gong (Wuhan University), Jianshuo Dong (Wuhan University), and Meng Xue (Wuhan University)*

SNAP: Efficient Extraction of Private Properties with Poisoning ........ 400
*Harsh Chaudhari (Northeastern University), John Abascal (Northeastern University), Alina Oprea (Northeastern University), Matthew Jagielski (Google Research), Florian Tramèr (ETH Zurich), and Jonathan Ullman (Northeastern University)*

On the (In)security of Peer-to-Peer Decentralized Machine Learning ........ 418
*Dario Pasquini (SPRING Lab; EPFL, Switzerland), Mathilde Raynal (SPRING Lab; EPFL, Switzerland), and Carmela Troncoso (SPRING Lab; EPFL, Switzerland)*

## Session 2C: SMC

Vectorized Batch Private Information Retrieval ........ 437
*Muhammad Haris Mughees (University of Illinois Urbana-Champaign, USA) and Ling Ren (University of Illinois Urbana-Champaign, USA)*

RoFL: Robustness of Secure Federated Learning ........ 453
*Hidde Lycklama (ETH Zurich), Lukas Burkhalter (ETH Zurich), Alexander Viand (ETH Zurich), Nicolas Küchler (ETH Zurich), and Anwar Hithnawi (ETH Zurich)*

Flamingo: Multi-Round Single-Server Secure Aggregation with Applications to Private Federated Learning ........ 477
*Yiping Ma (University of Pennsylvania), Jess Woods (University of Pennsylvania), Sebastian Angel (University of Pennsylvania, Microsoft Research), Antigoni Polychroniadou (JP Morgan AI Research), and Tal Rabin (University of Pennsylvania)*

SoK: Cryptographic Neural-Network Computation ........ 497
*Lucien K. L. Ng (Georgia Institute of Technology, USA) and Sherman S. M. Chow (The Chinese University of Hong Kong, Hong Kong)*

FLUTE: Fast and Secure Lookup Table Evaluations ........ 515
*Andreas Brüggemann (Technical University of Darmstadt), Robin Hundt (Technical University of Darmstadt), Thomas Schneider (Technical University of Darmstadt), Ajith Suresh (Technical University of Darmstadt), and Hossein Yalame (Technical University of Darmstadt)*

Bicoptor: Two-round Secure Three-party Non-linear Computation without Preprocessing for Privacy-preserving Machine Learning ........ 534
*Lijing Zhou (Huawei Technology, China), Ziyu Wang (Huawei Technology, China), Hongrui Cui (Shanghai Jiao Tong University, China), Qingrui Song (Huawei Technology, China), and Yu Yu (Shanghai Jiao Tong University, China)*

## Session 3A: Authentication

Investigating the Password Policy Practices of Website Administrators ...................................... 552
*Sena Sahin (Georgia Institute of Technology, USA), Suood Al Roomi (Georgia Institute of Technology, USA ; Kuwait University, Kuwait), Tara Poteat (Georgia Institute of Technology, USA), and Frank Li (Georgia Institute of Technology, USA)*

"In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya ................................................ 570
*Collins W. Munyendo (The George Washington University), Yasemin Acar (Paderborn University), and Adam J. Aviv (The George Washington University)*

Perceptions of Distributed Ledger Technology Key Management – An Interview Study with Finance Professionals ........................................................................................................ N/A
*Carolyn Guthoff (CISPA Helmholtz Center for Information Security, Germany, and Saarland University, Germany), Simon Anell (CISPA Helmholtz Center for Information Security, Germany, and Saarland University, Germany), Johann Hainzinger (Plutoneo Consulting GmbH, Germany), Adrian Dabrowski (CISPA Helmholtz Center for Information Security, Germany), and Katharina Krombholz (CISPA Helmholtz Center for Information Security, Germany)*

Towards a Rigorous Statistical Analysis of Empirical Password Datasets .................................... 606
*Jeremiah Blocki (Purdue University, USA) and Peiyuan Liu (Purdue University, USA)*

Confident Monte Carlo: Rigorous Analysis of Guessing Curves for Probabilistic Password Models ........................................................................................................ 626
*Peiyuan Liu (Purdue University, USA), Jeremiah Blocki (Purdue University, USA), and Wenjie Bai (Purdue University, USA)*

Not Yet Another Digital ID: Privacy-preserving Humanitarian Aid Distribution ......................... 645
*Boya Wang (EPFL), Wouter Lueks (CISPA Helmholtz Center for Information Security), Justinas Sukaitis (International Committee for the Red Cross), Vincent Graf Narbel (International Committee for the Red Cross), and Carmela Troncoso (EPFL)*

## Session 3B: Machine learning backdoors

Disguising Attacks with Explanation-Aware Backdoors ........................................................... 664
*Maximilian Noppel (KASTEL Security Research Labs, Karlsruhe Institute of Technology, Germany), Lukas Peter (KASTEL Security Research Labs, Karlsruhe Institute of Technology, Germany), and Christian Wressnegger (KASTEL Security Research Labs, Karlsruhe Institute of Technology, Germany)*

Selective Amnesia: On Efficient, High-Fidelity and Blind Suppression of Backdoor Effects in Trojaned Machine Learning Models ........................................................................... 682
*Rui Zhu (Indiana University Bloomington), Di Tang (Indiana University Bloomington), Siyuan Tang (Indiana University Bloomington), XiaoFeng Wang (Indiana University Bloomington), and Haixu Tang (Indiana University Bloomington)*

AI-Guardian: Defeating Adversarial Attacks using Backdoors .................................................. 701
*Hong Zhu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Shengzhi Zhang (Boston University, USA), and Kai Chen (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)*

Jigsaw Puzzle: Selective Backdoor Attack to Subvert Malware Classifiers .................................. 719
*Limin Yang (University of Illinois at Urbana-Champaign), Zhi Chen (University of Illinois at Urbana-Champaign), Jacopo Cortellazzi (King's College London and University College London), Feargus Pendlebury (University College London), Kevin Tu (University of Illinois at Urbana-Champaign), Fabio Pierazzi (King's College London), Lorenzo Cavallaro (University College London), and Gang Wang (University of Illinois at Urbana-Champaign)*

BayBFed: Bayesian Backdoor Defense for Federated Learning .................................................. 737
*Kavita Kumari (Technical University of Darmstadt, Germany), Phillip Rieger (Technical University of Darmstadt, Germany), Hossein Fereidooni (Technical University of Darmstadt, Germany), Murtuza Jadliwala (The University of Texas at San Antonio, United States), and Ahmad-Reza Sadeghi (Technical University of Darmstadt, Germany)*

REDEEM MYSELF: Purifying Backdoors in Deep Learning Models using Self Attention Distillation .................................................. 755
*Xueluan Gong (School of Computer Science, Wuhan University, China), Yanjiao Chen (College of Electrical Engineering, Zhejiang University, China), Wang Yang (School of Cyber Science and Engineering, Wuhan University, China), Qian Wang (School of Cyber Science and Engineering, Wuhan University, China), Yuzhe Gu (School of Cyber Science and Engineering, Wuhan University, China), Huayang Huang (School of Cyber Science and Engineering, Wuhan University, China), and Chao Shen (School of Cyber Science and Engineering, Xi'an Jiaotong University, China)*

## Session 3C: Cryptographic protocols

Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance ..............................773
*Jack Doerner (Technion), Yashvanth Kondi (Aarhus University), Eysa Lee (Northeastern University), Abhi Shelat (Northeastern University), and LaKyah Tyner (Northeastern University)*

zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure ..................................................790
*Michael Rosenberg (University of Maryland), Jacob White (Purdue University), Christina Garman (Purdue University), and Ian Miers (University of Maryland)*

Private Access Control for Function Secret Sharing .................................................. 809
*Sacha Servan-Schreiber (MIT CSAIL), Simon Beyzerov (MIT PRIMES), Eli Yablon (MIT PRIMES), and Hyojae Park (MIT PRIMES)*

MPCAuth: Multi-factor Authentication for Distributed-trust Systems ........................................ 829
*Sijun Tan (UC Berkeley), Weikeng Chen (UC Berkeley), Ryan Deng (UC Berkeley), and Raluca Ada Popa (UC Berkeley)*

Silph: A Framework for Scalable and Accurate Generation of Hybrid MPC Protocols .................. 848
*Edward Chen (Carnegie Mellon University; Stanford University), Jinhao Zhu (Carnegie Mellon University), Alex Ozdemir (Stanford Univesity), Riad Wahby (Carnegie Mellon University), Fraser Brown (Carnegie Mellon University), and Wenting Zheng (Carnegie Mellon University)*

## Session 4A: Biometric security

SoK: Anti-Facial Recognition Technology .......................................................................... 864
*Emily Wenger (University of Chicago), Shawn Shan (University of Chicago), Haitao Zheng (University of Chicago), and Ben Y. Zhao (University of Chicago)*

Spoofing Real-world Face Authentication Systems through Optical Synthesis ............................. 882
*Yueli Yan (School of Information Science and Technology, ShanghaiTech University, China) and Zhice Yang (School of Information Science and Technology, ShanghaiTech University, China)*

ImU: Physical Impersonating Attack for Face Recognition System with Natural Style Changes ...... 899
*Shengwei An (Purdue University, USA), Yuan Yao (Nanjing University, China), Qiuling Xu (Purdue University, USA), Shiqing Ma (Rutgers University, USA), Guanhong Tao (Purdue University, USA), Siyuan Cheng (Purdue University, USA), Kaiyuan Zhang (Purdue University, USA), Yingqi Liu (Purdue University, USA), Guangyu Shen (Purdue University, USA), Ian Kelk (Clarifai Inc., USA), and Xiangyu Zhang (Purdue University, USA)*

DepthFake: Spoofing 3D Face Authentication with a 2D Photo ................................................. 917
*Zhihao Wu (Zhejiang University, China), Yushi Cheng (Tsinghua University, China), Jiahui Yang (Zhejiang University, China), Xiaoyu Ji (Zhejiang University, China), and Wenyuan Xu (Zhejiang University, China)*

Understanding the (In)Security of Cross-side Face Verification Systems in Mobile Apps: A System Perspective ............................................................................................................ 934
*Xiaohan Zhang (Fudan University, China), Haoqi Ye (Fudan University, China), Ziqi Huang (Fudan University, China), Xiao Ye (Fudan University, China), Yinzhi Cao (Johns Hopkins University, USA), Yuan Zhang (Fudan University, China), and Min Yang (Fudan University, China)*

Breaking Security-Critical Voice Authentication .................................................................... 951
*Andre Kassis (University of Waterloo, Canada) and Urs Hengartner (University of Waterloo, Canada)*

## Session 4B: Web security

SoK: A Critical Evaluation of Efficient Website Fingerprinting Defenses .................................... 969
*Nate Mathews (Rochester Institute of Technology), James K Holland (University of Minnesota), Se Eun Oh (Ewha Womans University), Mohammad Saidur Rahman (Rochester Institute of Technology), Nicholas Hopper (University of Minnesota), and Matthew Wright (Rochester Institute of Technology)*

Fashion Faux Pas: Implicit Stylistic Fingerprints for Bypassing Browsers' Anti-Fingerprinting Defenses ........ 987
*Xu Lin (University of Illinois Chicago, United States), Frederico Araujo (IBM Research, United States), Teryl Taylor (IBM Research, United States), Jiyong Jang (IBM Research, United States), and Jason Polakis (University of Illinois Chicago, United States)*

Robust Multi-tab Website Fingerprinting Attacks in the Wild ........ 1005
*Xinhao Deng (Tsinghua University, China), Qilei Yin (Zhongguancun Laboratory, China), Zhuotao Liu (Tsinghua University, China), Xiyuan Zhao (Tsinghua University, China), Qi Li (Tsinghua University, China), Mingwei Xu (Tsinghua University, China), Ke Xu (Tsinghua University, Beijing), and Jianping Wu (Tsinghua University, China)*

Only Pay for What You Leak: Leveraging Sandboxes for a Minimally Invasive Browser Fingerprinting Defense ........1023
*Ryan Torok (Princeton University) and Amit Levy (Princeton University)*

It’s (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defenses ........ 1041
*Soheil Khodayari (CISPA Helmholtz Center for Information Security, Germany) and Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany)*

Scaling JavaScript Abstract Interpretation to Detect and Exploit Node.js Taint-style Vulnerability ........1059
*Mingqing Kang (Johns Hopkins University), Yichao Xu (Johns Hopkins University), Song Li (Zhejiang University), Rigel Gjomemo (University of Illinois Chicago), Jianwei Hou (Renmin University of China), V.N. Venkatakrishnan (University of Illinois Chicago), and Yinzhi Cao (Johns Hopkins University)*

## Session 4C: Cryptographic proof techniques

Sound Verification of Security Protocols: From Design to Interoperable Implementations ........ 1077
*Linard Arquint (ETH Zurich, Switzerland), Felix A. Wolf (ETH Zurich, Switzerland), Joseph Lallemand (Univ Rennes, CNRS, IRISA, France), Ralf Sasse (ETH Zurich, Switzerland), Christoph Sprenger (ETH Zurich, Switzerland), Sven N. Wiesner (ETH Zurich, Switzerland), David Basin (ETH Zurich, Switzerland), and Peter Müller (ETH Zurich, Switzerland)*

Typing High-Speed Cryptography against Spectre v1 ........1094
*Basavesh Ammanaghatta Shivakumar (MPI-SP), Gilles Barthe (MPI-SP and IMDEA Software Institute), Benjamin Grégoire (Inria and Université Côte d’Azur), Vincent Laporte (Université de Lorraine, CNRS and Inria), Tiago Oliviera (MPI-SP), Swarn Priya (Inria and Université Côte d’Azur), Peter Schwabe (MPI-SP & Radboud University), and Lucas Tabary-Maujean (ENS Paris-Saclay)*

Less is more: refinement proofs for probabilistic proofs ........1112
*Kunming Jiang (NYU and Carnegie Mellon), Devora Chait-Roth (NYU), Zachary DeStefano (NYU), Michael Walfish (NYU), and Thomas Wies (NYU)*

OWL: Compositional Verification of Security Protocols via an Information-Flow Type System ..... 1130
*Joshua Gancher (Carnegie Mellon University, USA), Sydney Gibson (Carnegie Mellon University, USA), Pratap Singh (Carnegie Mellon University, USA), Samvid Dharanikota (Carnegie Mellon University, USA), and Bryan Parno (Carnegie Mellon University, USA)*

AUC: Accountable Universal Composability ..... 1148
*Mike Graf (University of Stuttgart), Ralf Küsters (University of Stuttgart), and Daniel Rausch (University of Stuttgart)*

High-Order Masking of Lattice Signatures in Quasilinear Time ..... 1168
*Rafaël del Pino (PQShield SAS, France), Thomas Prest (PQShield SAS, France), Mélissa Rossi (ANSSI, France), and Markku-Juhani Saarinen (PQShield LTD, UK)*

## Session 5A: Software security

Practical Timing Side-Channel Attacks on Memory Compression ..... 1186
*Martin Schwarzl (Graz University of Technology), Pietro Borrello (Sapienza University of Rome), Gururaj Saileshwar (NVIDIA Research), Hanna Müller (Graz University of Technology), Michael Schwarz (CISPA Helmholtz Center for Information Security), and Daniel Gruss (Graz University of Technology)*

TEEzz: Fuzzing Trusted Applications on COTS Android Devices ..... 1204
*Marcel Busch (EPFL), Aravind Machiry (Purdue University), Chad Spensky (Allthenticate), Giovanni Vigna (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara), and Mathias Payer (EPFL)*

Half&Half: Demystifying Intel’s Directional Branch Predictors for Fast, Secure Partitioned Execution ..... 1220
*Hosein Yavarzadeh (University of California San Diego), Mohammadkazem Taram (Purdue University), Shravan Narayan (University of California San Diego), Deian Stefan (University of California San Diego), and Dean Tullsen (University of California San Diego)*

Improving Developers' Understanding of Regex Denial of Service Tools through Anti-Patterns and Fix Strategies ..... 1238
*Sk Adnan Hassan (Virginia Tech, USA), Zainab Aamir (Stony Brook University, USA), Dongyoon Lee (Stony Brook University, USA), James C. Davis (Purdue University, USA), and Francisco Servant (University of Málaga, Spain)*

Practical Program Modularization with Type-Based Dependence Analysis ..... 1256
*Kangjie Lu (University of Minnesota)*

WarpAttack: Bypassing CFI through Compiler-Introduced Double-Fetches ..... 1271
*Jianhao Xu (Nanjing University, China), Luca Di Bartolomeo (EPFL, Switzerland), Flavio Toffalini (EPFL, Switzerland), Bing Mao (Nanjing University, China), and Mathias Payer (EPFL, Switzerland)*

## Session 5B: Machine learning assurance

SoK: Certified Robustness for Deep Neural Networks ..... 1289
*Linyi Li (University of Illinois Urbana-Champaign, USA), Tao Xie (Key Laboratory of High Confidence Software Technologies, MoE (Peking University), China), and Bo Li (University of Illinois Urbana-Champaign, USA)*

RAB: Provable Robustness Against Backdoor Attacks ..... 1311
*Maurice Weber (ETH Zurich, Switzerland), Xiaojun Xu (University of Illinois at Urbana-Champaign, USA), Bojan Karlas (ETH Zurich, Switzerland), Ce Zhang (ETH Zurich, Switzerland), and Bo Li (University of Illinois at Urbana-Champaign, USA)*

ObjectSeeker: Certifiably Robust Object Detection against Patch Hiding Attacks via Patch-agnostic Masking ..... 1329
*Chong Xiang (Princeton University), Alexander Valtchanov (Princeton University), Saeed Mahloujifar (Princeton University), and Prateek Mittal (Princeton University)*

PublicCheck: Public Integrity Verification for Services of Run-time Deep Models ..... 1348
*Shuo Wang (CSIRO's Data61, Australia; Cybersecurity CRC, Australia), Sharif Abuadbba (CSIRO's Data61, Australia; Cybersecurity CRC, Australia), Sidharth Agarwal (Indian Institute of Technology Delhi, India), Kristen Moore (CSIRO's Data61, Australia; Cybersecurity CRC, Australia), Ruoxi Sun (CSIRO's Data61, Australia), Minhui Xue (CSIRO's Data61, Australia; Cybersecurity CRC, Australia), Surya Nepal (CSIRO's Data61, Australia; Cybersecurity CRC, Australia), Seyit Camtepe (CSIRO's Data61, Australia; Cybersecurity CRC, Australia), and Salil Kanhere (University of New South Wales, Australia)*

FedRecover: Recovering from Poisoning Attacks in Federated Learning using Historical Information ..... 1366
*Xiaoyu Cao (Duke University), Jinyuan Jia (Duke University), Zaixi Zhang (University of Science and Technology of China), and Neil Zhenqiang Gong (Duke University)*

On The Empirical Effectiveness of Unrealistic Adversarial Hardening Against Realistic Adversarial Attacks ..... 1384
*Salijona Dyrmishi (University of Luxembourg, Luxembourg), Salah Ghamizi (University of Luxembourg, Luxembourg), Thibault Simonetto (University of Luxembourg, Luxembourg), Yves Le Traon (University of Luxembourg, Luxembourg), and Maxime Cordy (University of Luxembourg, Luxembourg)*

## Session 5C: Applied cryptography

Rethinking Searchable Symmetric Encryption ..... 1401
*Zichen Gui (ETH Zurich, Switzerland), Kenneth G. Paterson (ETH Zurich, Switzerland), and Sikhar Patranabis (IBM Research, India)*

Private Collaborative Data Cleaning via Non-Equi PSI ..... 1419
*Erik-Oliver Blass (Airbus, Germany) and Florian Kerschbaum (University of Waterloo, Canada)*

SPHINCS+C: Compressing SPHINCS+ With (Almost) No Cost ........ 1435
*Andreas Hülsing (TU Eindhoven), Mikhail Kudinov (TU Eindhoven), Eyal Ronen (Tel Aviv University), and Eylon Yogev (Bar-Ilan University)*

Threshold Signatures in the Multiverse ........ 1454
*Leemon Baird (Swirlds Labs), Sanjam Garg (University of California, Berkeley&NTT Research), Abhishek Jain (Johns Hopkins University), Pratyay Mukherjee (Supra Oracles), Rohit Sinha (Meta), Mingyuan Wang (University of California, Berkeley), and Yinuo Zhang (University of California, Berkeley)*

FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation ........ 1471
*Nina Bindel (SandboxAQ), Cas Cremers (CISPA Helmholtz Center for Information Security), and Mang Zhao (CISPA Helmholtz Center for Information Security)*

Token meets Wallet: Formalizing Privacy and Revocation for FIDO2 ........ 1491
*Lucjan Hanzlik (CISPA Helmholtz Center for Information Security, Germany), Julian Loss (CISPA Helmholtz Center for Information Security, Germany), and Benedikt Wagner (CISPA Helmholtz Center for Information Security, Germany and Saarland University, Germany)*

## Session 6A: Software supply chains

SoK: Taxonomy of Attacks on Open-Source Software Supply Chains ........ 1509
*Piergiorgio Ladisa (SAP Security Research,  Université de Rennes 1), Henrik Plate (SAP Security Research), Matias Martinez (Université Polytechnique Hauts-de-France), and Olivier Barais (Université de Rennes 1, Inria, IRISA)*

It’s like flossing your teeth: On the Importance and Challenges of Reproducible Builds for Software Supply Chain Security ........ 1527
*Marcel Fourné (Max Planck Institute for Security and Privacy, Bochum, Germany), Dominik Wermke (CISPA Helmholtz Center for Information Security, Germany), William Enck (North Carolina State University, Raleigh, North Carolina, USA), Sascha Fahl (CISPA Helmholtz Center for Information Security, Germany), and Yasemin Acar (Paderborn University, Germany, George Washington University, USA)*

"Always Contribute Back": A Qualitative Study on Security Challenges of the Open Source Supply Chain ........ 1545
*Dominik Wermke (CISPA Helmholtz Center for Information Security), Jan H. Klemmer (Leibniz University Hannover), Noah Wöhler (CISPA Helmholtz Center for Information Security), Juliane Schmüser (CISPA Helmholtz Center for Information Security), Harshini Sri Ramulu (Paderborn University), Yasemin Acar (Paderborn University, George Washington University), and Sascha Fahl (CISPA Helmholtz Center for Information Security, Leibniz University Hannover)*

Continuous Intrusion: Characterizing the Security of Continuous Integration Services ................ 1561
*Yacong Gu (Qi An Xin Technology Research Institute, China), Lingyun Ying (Qi An Xin Technology Research Institute, China), Huajun Chai (Qi An Xin Technology Research Institute, China), Chu Qiao (University of Delaware, USA), Haixin Duan (Tsinghua University; Tsinghua University-QI-ANXIN Group JCNS, China), and Xing Gao (University of Delaware, USA)*

Investigating Package Related Security Threats in Software Registries ...................................... 1578
*Yacong Gu (QI-ANXIN Technology Research Institute, China), Lingyun Ying (QI-ANXIN Technology Research Institute, China), Yingyuan Pu (Ocean University of China; QI-ANXIN Technology Research Institute, China), Xiao Hu (QI-ANXIN Technology Research Institute, China), Huajun Chai (QI-ANXIN Technology Research Institute, China), Ruimin Wang (Southeast University; QI-ANXIN Technology Research Institute, China), Xing Gao (University of Delaware, USA), and Haixin Duan (Tsinghua University; Tsinghua University-QI-ANXIN Group JCNS, China)*

## Session 6B: ML attacks

ShadowNet: A Secure and Efficient On-device Model Inference System for Convolutional Neural Networks ........................................................................................................ 1596
*Zhichuang Sun (Google), Ruimin Sun (Florida International University), Changming Liu (Northeastern University), Amrita Roy Chowdhury (University of California, San Diego), Long Lu (Northeastern University), and Somesh Jha (University of Wisconsin-Madison)*

Deepfake Text Detection: Limitations and Opportunities ........................................................ 1613
*Jiameng Pu (Virginia Tech, USA), Zain Sarwar (University Of Chicago, USA), Sifat Muhammad Abdullah (Virginia Tech, USA), Abdullah Rehman (Virginia Tech, USA), Yoonjin Kim (Virginia Tech, USA), Parantapa Bhattacharya (University Of Virginia, USA), Mobin Javed (LUMS, Pakistan), and Bimal Viswanath (Virginia Tech, USA)*

StyleFool: Fooling Video Classification Systems via Style Transfer ........................................... 1631
*Yuxin Cao (Shenzhen International Graduate School, Tsinghua University, China), Xi Xiao (Shenzhen International Graduate School, Tsinghua University, China), Ruoxi Sun (CSIRO's Data61, Australia), Derui Wang (CSIRO's Data61, Australia), Minhui Xue (CSIRO's Data61, Australia), and Sheng Wen (Swinburne University of Technology, Australia)*

GeeSolver: A Generic, Efficient, and Effortless Solver with Self-Supervised Learning for Breaking Text Captchas ........................................................................................... 1649
*Ruijie Zhao (Shanghai Jiao Tong University), Xianwen Deng (Shanghai Jiao Tong University), Yanhao Wang (QI-ANXIN), Zhicong Yan (Shanghai Jiao Tong University), Zhengguang Han (QI-AN Pangu (Shanghai) InfoTech Co., Ltd.), Libo Chen (Shanghai Jiao Tong University), Zhi Xue (Shanghai Jiao Tong University), and Yijun Wang (Shanghai Jiao Tong University)*

TrojanModel: A Practical Trojan Attack against Automatic Speech Recognition Systems .............1667
*Wei Zong (University of Wollongong, Australia), Yang-Wai Chow (University of Wollongong, Australia), Willy Susilo (University of Wollongong, Australia), Kien Do (Deakin University, Australia), and Svetha Venkatesh (Deakin University, Australia)*

## Session 6C: Rowhammer and spectre

REGA: Scalable Rowhammer Mitigation with Refresh-Generating Activations .......................... 1684
*Michele Marazzi (ETH Zurich), Flavien Solt (ETH Zurich), Patrick Jattke (ETH Zurich), Kubo Takashi (Zentel Japan), and Kaveh Razavi (ETH Zurich)*

CSI:Rowhammer - Cryptographic Security and Integrity against Rowhammer .......................... 1702
*Jonas Juffinger (Lamarr Security Research, Graz University of Technology, Austria), Lukas Lamster (Graz University of Technology, Austria), Andreas Kogler (Graz University of Technology, Austria), Maria Eichlseder (Graz University of Technology, Austria), Moritz Lipp (Amazon Web Services, Austria), and Daniel Gruss (Graz University of Technology, Austria)*

Jolt: Recovering TLS Signing Keys via Rowhammer Faults ...................................................... 1719
*Koksal Mus (Worcester Polytechnic Institute), Yarkın Doröz (Worcester Polytechnic Institute), M. Caner Tol (Worcester Polytechnic Institute), Kristi Rahman (Worcester Polytechnic Institute), and Berk Sunar (Worcester Polytechnic Institute)*

Hide and Seek with Spectres: Efficient discovery of speculative information leaks with random testing ........................................................................................................ 1737
*Oleksii Oleksenko (Microsoft Research), Marco Guarnieri (IMDEA Software Institute), Boris Kopf (Microsoft Research), and Mark Silberstein (Technion)*

Spectre Declassified: Reading from the Right Place at the Wrong Time .................................... 1753
*Basavesh Ammanaghatta Shivakumar (Max Planck Institute for Security and Privacy, Germany), Jack Barnes (The University of Adelaide, Australia), Gilles Barthe (Max Planck Institute for Security and Privacy, Germany; IMDEA Software Institute, Spain), Sunjay Cauligi (Max Planck Institute for Security and Privacy, Germany), Chitchanok Chuengsatiansup (The University of Adelaide, Australia), Daniel Genkin (Georgia Institute of Technology, USA), Sioli O'Connell (The University of Adelaide, Australia), Peter Schwabe (Max Planck Institute for Security and Privacy, Germany; Radboud University, Netherlands), Rui Qi Sim (The University of Adelaide, Australia), and Yuval Yarom (The University of Adelaide, Australia)*

## Session 7A: Physical channel attacks

Volttack: Control IoT Devices by Manipulating Power Supply Voltage ..................................... 1771
*Kai Wang (Zhejiang University, China), Shilin Xiao (Zhejiang University, China), Xiaoyu Ji (Zhejiang University, China), Chen Yan (Zhejiang University, China), Chaohao Li (Hangzhou Hikvision Digital Technology Co., Ltd., China), and Wenyuan Xu (Zhejiang University, China)*

Inducing Wireless Chargers to Voice Out for Inaudible Command Attacks ............................... 1789
*Donghui Dai (The Hong Kong Polytechnic University, China), Zhenlin An (The Hong Kong Polytechnic University, China), and Lei Yang (The Hong Kong Polytechnic University, China)*

mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array .......... 1807
*Rohith Reddy Vennam (University of California San Diego), Ish Kumar Jain (University of California San Diego), Kshitiz Bansal (University of California San Diego), Joshua Orozco (University of California San Diego), Puja Shukla (University of California San Diego), Aanjhan Ranganathan (Northeastern University), and Dinesh Bharadia (University of California San Diego)*

PLA-LiDAR: Physical Laser Attacks against LiDAR-based 3D Object Detection in Autonomous Vehicle ........................................................................................................ 1822
*Zizhi Jin (Zhejiang University), Ji Xiaoyu (Zhejiang University), Yushi Cheng (Tsinghua University), Bo Yang (Zhejiang University), Chen Yan (Zhejiang University), and Wenyuan Xu (Zhejiang University)*

mmEcho: A mmWave-based Acoustic Eavesdropping Method ................................................ 1840
*Pengfei Hu (Shandong University), Wenhao Li (Shandong University), Riccardo Spolaor (Shandong University), and Xiuzhen Cheng (Shandong University)*

Side Eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses ......................................................................... 1857
*Yan Long (University of Michigan, USA), Pirouz Naghavi (University of Florida, USA), Blas Kojusner (University of Florida, USA), Kevin Butler (University of Florida, USA), Sara Rampazzi (University of Florida, USA), and Kevin Fu (University of Michigan, USA)*

## Session 7B: ML Security and Privacy

ADI: Adversarial Dominating Inputs in Vertical Federated Learning Systems ........................... 1875
*Qi Pang (Carnegie Mellon University, USA), Yuanyuan Yuan (Hong Kong University of Science and Technology, Hong Kong SAR), Shuai Wang (Hong Kong University of Science and Technology, Hong Kong SAR), and Wenting Zheng (Carnegie Mellon University, USA)*

3DFed: Adaptive and Extensible Framework for Covert Backdoor Attack in Federated Learning .. 1893
*Haoyang LI (The Hong Kong Polytechnic University), Qingqing Ye (The Hong Kong Polytechnic University), Haibo Hu (The Hong Kong Polytechnic University), Jin Li (Guangzhou University), Leixia Wang (Renmin University of China), Chengfang Fang (Huawei International, Singapore), and Jie Shi (Huawei International, Singapore)*

Scalable and Privacy-Preserving Federated Principal Component Analysis ............................... 1908
*David Froelicher (MIT, USA), Hyunghoon Cho (Broad Institute of MIT and Harvard, USA), Manaswitha Edupalli (Broad Institute of MIT and Harvard, USA), Joao Sa Sousa (EPFL, Switzerland), Jean-Philippe Bossuat (Tune Insight SA, Switzerland), Apostolos Pyrgelis (EPFL, Switzerland), Juan R. Troncoso-Pastoriza (Tune Insight SA, Switzerland), Bonnie Berger (MIT, USA), and Jean-Pierre Hubaux (EPFL, Switzerland)*

Private, Efficient, and Accurate: Protecting Models Trained by Multi-party Learning with Differential Privacy ............................................................ 1926
*Wenqiang Ruan (Fudan University, China), Mingxin Xu (Fudan University, China), Wenjing Fang (Ant Group, China), Li Wang (Ant Group, China), Lei Wang (Ant Group, China), and Weili Han (Fudan University, China)*

Spectral-DP: Differentially Private Deep Learning through Spectral Perturbation and Filtering ............................................................ 1944
*Ce Feng (Lehigh University), Nuo Xu (Lehigh University), Wujie Wen (Lehigh University), Parv Venkitasubramaniam (Lehigh University), and Caiwen Ding (University of Connecticut)*

ELSA: Secure Aggregation for Federated Learning with Malicious Actors ................................ 1961
*Mayank Rathee (University of California, Berkeley, USA), Conghao Shen (Stanford University, USA), Sameer Wagh (Devron Corporation, USA), and Raluca Ada Popa (University of California, Berkeley, USA)*

## Session 7C: Human factors

No One Drinks From the Firehose: How Organizations Filter and Prioritize Vulnerability Information ............................................................ 1980
*Stephanie de Smale (National Cyber Security Centre, The Netherlands & Delft University of Technology, The Netherlands), Rik van Dijk (National Cyber Security Centre, The Netherlands), Xander Bouwman (Delft University of Technology, The Netherlands), Jeroen van der Ham (National Cyber Security Centre, The Netherlands & University of Twente, The Netherlands), and Michel van Eeten (Delft University of Technology, The Netherlands)*

Vulnerability Discovery for All: Experiences of Marginalization in Vulnerability Discovery......... 1997
*Kelsey R. Fulton (University of Maryland), Samantha Katcher (Tufts University), Kevin Song (University of Chicago), Marshini Chetty (University of Chicago), Michelle L. Mazurek (University of Maryland), Daniel Votipka (Tufts University), and Chloé Messdaghi (Impactive Consulting)*

"We are a startup to the core":   A qualitative interview study on the security and privacy development practices in Turkish software startups ................................................... 2015
*Dilara Kekulluoglu (University of Edinburgh, UK) and Yasemin Acar (The George Washington University, USA)*

"How technical do you get? I'm an English teacher": Teaching and Learning Cybersecurity and AI Ethics in High School ........ 2032
*Zachary Kilhoffer (University of Illinois at Urbana-Champaign, USA), Zhixuan Zhou (University of Illinois at Urbana-Champaign, USA), Firmiana Wang (University of Illinois Laboratory High School, USA), Fahad Tamton (University of Illinois at Urbana-Champaign, USA), Yun Huang (University of Illinois at Urbana-Champaign, USA), Pilyoung Kim (University of Denver, USA), Tom Yeh (University of Colorado Boulder, USA), and Yang Wang (University of Illinois at Urbana-Champaign, USA)*

Skilled or Gullible? Gender Stereotypes Related to Computer Security and Privacy ........ 2050
*Miranda Wei (University of Washington, USA), Pardis Emami-Naeini (Duke University, USA), Franziska Roesner (University of Washington, USA), and Tadayoshi Kohno (University of Washington, USA)*

Everybody’s Got ML, Tell Me What Else You Have: Practitioners' Perception of ML-Based Security Tools and Explanations ........ 2068
*Jaron Mink (University of Illinois at Urbana-Champaign), Hadjer Benkraouda (University of Illinois at Urbana-Champaign), Limin Yang (University of Illinois at Urbana-Champaign), Arridhana Ciptadi (Truera), Ali Ahmadzadeh (Blue Hexagon), Daniel Votipka (Tufts University), and Gang Wang (University of Illinois at Urbana-Champaign)*

## Session 8A: Low-level software security

Precise Detection of Kernel Data Races with Probabilistic Lockset Analysis ........ 2086
*Gabriel Ryan (Columbia University), Abhishek Shah (Columbia University), Dongdong She (Columbia University), and Suman Jana (Columbia University)*

SEGFUZZ: Segmentizing Thread Interleaving to Discover Kernel Concurrency Bugs through Fuzzing ........ 2104
*Dae R. Jeong (School of Computing, KAIST), Byoungyoung Lee (Department of Electrical and Computer Engineering, Seoul National University), Insik Shin (School of Computing, KAIST), and Youngjin Kwon (School of Computing, KAIST)*

AEM: Facilitating Cross-Version Exploitability Assessment of Linux Kernel Vulnerabilities ........ 2122
*Zheyue Jiang (Fudan University), Yuan Zhang (Fudan University), Jun Xu (University of Utah), Xinqian Sun (Fudan University), Zhuang Liu (Fudan University), and Min Yang (Fudan University)*

When Top-down Meets Bottom-up: Detecting and Exploiting Use-After-Cleanup Bugs in Linux Kernel ........ 2138
*Lin Ma (Zhejiang University, China), Duoming Zhou (Zhejiang University, China), Hanjie Wu (Carnegie Mellon University, USA), Yajin Zhou (Zhejiang University, China), Rui Chang (Zhejiang University, China), Hao Xiong (Zhejiang University, China), Lei Wu (Zhejiang University, China), and Kui Ren (Zhejiang University, China)*

RSFuzzer: Discovering Deep SMI Handler Vulnerabilities in UEFI Firmware with Hybrid Fuzzing ........ 2155
*Jiawei Yin (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), Menghao Li (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), Yuekang Li (Nanyang Technological University), Yong Yu (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), Boru Lin (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), Yanyan zou (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), Yang Liu (Nanyang Technological University), Wei Huo (nstitute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), and Jingling Xue (UNSW Sydney)*

## Session 8B: Privacy and covert channels

A Theory to Instruct Differentially-Private Learning via Clipping Bias Reduction ........ 2170
*Hanshen Xiao (MIT), Zihang Xiang (KAUST), Di Wang (KAUST), and Srinivas Devadas (MIT)*

Continual Observation under User-level Differential Privacy ........ 2190
*Wei Dong (Hong Kong University of Science and Technology, China), Qiyao Luo (Hong Kong University of Science and Technology, China), and Ke Yi (Hong Kong University of Science and Technology, China)*

Locally Differentially Private Frequency Estimation Based on Convolution Framework ........ 2208
*Huiyu Fang (Southeast University), Liquan Chen (Southeast University), Yali Liu (Jiangsu Normal University), and Yuan Gao (Southeast University)*

TELEPATH: A Minecraft-based Covert Communication System ........ 2223
*Zhen Sun (Cornell Tech) and Vitaly Shmatikov (Cornell Tech)*

Discop: Provably Secure Steganography in Practice Based on “Distribution Copies” .................. 2238
*Jinyang Ding (University of Science and Technology of China, China), Kejiang Chen (University of Science and Technology of China, China), Yaofei Wang (Hefei University of Technology, China), Na Zhao (University of Science and Technology of China, China), Weiming Zhang (University of Science and Technology of China, China), and Nenghai Yu (University of Science and Technology of China, China)*

## Session 8C: Side-channel attacks

SQUIP: Exploiting the Scheduler Queue Contention Side Channel ........................................... 2256
*Stefan Gast (Lamarr Security Research, Graz University of Technology), Jonas Juffinger (Lamarr Security Research, Graz University of Technology), Martin Schwarzl (Graz University of Technology), Gururaj Saileshwar (Georgia Institute of Technology), Andreas Kogler (Graz University of Technology), Simone Franza (Graz University of Technology), Markus Köstl (Graz University of Technology), and Daniel Gruss (Lamarr Security Research, Graz University of Technology)*

Scatter and Split Securely: Defeating Cache Contention and Occupancy Attacks ......................... 2273
*Lukas Giner (Graz University of Technology, Austria), Stefan Steinegger (Graz University of Technology, Austria), Antoon Purnal (Ku Leuven, Belgium), Maria Eichlseder (Graz University of Technology, Austria), Thomas Unterluggauer (Intel Corporation), Stefan Mangard (Graz University of Technology, Austria), and Daniel Gruss (Graz University of Technology, Austria)*

DEVIOUS: Device-Driven Side-Channel Attacks on the IOMMU ............................................. 2288
*Taehun Kim (Korea University, Republic of Korea), Hyeongjin Park (Korea University, Republic of Korea), Seokmin Lee (Korea University, Republic of Korea), Seunghee Shin (The State University of New York at Binghamton, USA), Junbeom Hur (Korea University, Republic of Korea), and Youngjoo Shin (Korea University, Republic of Korea)*

DVFS Frequently Leaks Secrets: Hertzbleed Attacks Beyond SIKE, Cryptography, and CPU-Only Data ............................................................................................................................ 2306
*Yingchen Wang (University of Texas at Austin), Riccardo Paccagnella (University of Illinois Urbana-Champaign, USA), Alan Wandke (University of Illinois Urbana-Champaign), Zhao Gang (University of Texas at Austin), Grant Garrett-Grossman (University of Illinois Urbana-Champaign), Christopher W. Fletcher (University of Illinois Urbana-Champaign), David Kohlbrenner (University of Washington), and Hovav Shacham (University of Texas at Austin)*

A Security RISC: Microarchitectural Attacks on Hardware RISC-V CPUs .................................. 2321
*Lukas Gerlach (CISPA Helmholtz Center for Information Security), Daniel Weber (CISPA Helmholtz Center for Information Security), Ruiyi Zhang (CISPA Helmholtz Center for Information Security), and Michael Schwarz (CISPA Helmholtz Center for Information Security)*

## Session 9A: Model-based software security

Examining Zero-Shot Vulnerability Repair with Large Language Models ..................................2339
*Hammond Pearce (New York University), Benjamin Tan (University of Calgary), Baleegh Ahmad (New York University), Ramesh Karri (New York University), and Brendan Dolan-Gavitt (New York University)*

Callee: Recovering Call Graphs for Binaries with Transfer and Contrastive Learning .................. 2357
*Wenyu Zhu (Tsinghua University & BNRist, China), Zhiyao Feng (Tsinghua University & BNRist, China), Zihan Zhang (Tsinghua University & BNRist, China), Jianjun Chen (Tsinghua University & Zhongguancun Laboratory, China), Zhijian Ou (Tsinghua University, China), Min Yang (Fudan University, China), and Chao Zhang (Tsinghua University & BNRist & Zhongguancun Laboratory, China)*

XFL: Naming Functions in Binaries with Extreme Multi-label Learning .................................... 2375
*James Patrick-Evans (Royal Holloway, University of London), Moritz Dannehl (Bundeswehr University Munich), and Johannes Kinder (Bundeswehr University Munich)*

D-ARM: Disassembling ARM Binaries by Lightweight Superset Instruction Interpretation and Graph Modeling ................................................................................................................ 2391
*Yapeng Ye (Purdue University, USA), Zhuo Zhang (Purdue University, USA), Qingkai Shi (Purdue University, USA), Yousra Aafer (University of Waterloo, Canada), and Xiangyu Zhang (Purdue University, USA)*

GraphSPD: Graph-Based Security Patch Detection with Enriched Code Semantics ...................... 2409
*Shu Wang (George Mason University, USA), Xinda Wang (George Mason University, USA), Kun Sun (George Mason University, USA), Sushil Jajodia (George Mason University, USA), Haining Wang (Virginia Tech, USA), and Qi Li (Tsinghua University, China)*

Effective ReDoS Detection by Principled Vulnerability Modeling and Exploit Generation ........... 2427
*Xinyi Wang (Institute of Information Engineering, Chinese Academy of Sciences, China), Cen Zhang (Nanyang Technological University), Yeting Li (Institute of Information Engineering, Chinese Academy of Sciences, China), Zhiwu Xu (Shenzhen University), Shuailin Huang (Institute of Information Engineering, Chinese Academy of Sciences, China), Yi Liu (Nanyang Technological University), Yican Yao (Institute of Information Engineering, Chinese Academy of Sciences, China), Yang Xiao (Institute of Information Engineering, Chinese Academy of Sciences, China), Yanyan Zou (Institute of Information Engineering, Chinese Academy of Sciences, China), Yang Liu (Institute of Information Engineering, Chinese Academy of Sciences, China), and Wei Huo (Institute of Information Engineering, Chinese Academy of Sciences, China)*

## Session 9B: Blockchain 2

SoK: Decentralized Finance (DeFi) Incidents ........ 2444
*Liyi Zhou (Imperial College London), Xihan Xiong (Imperial College London), Jens Ernstberger (Technical University of Munich), Stefanos Chaliasos (Imperial College London), Zhipeng Wang (Imperial College London), Ye Wang (University of Macau), Kaihua Qin (Imperial College London), Roger Wattenhofer (ETH Zurich), Dawn Song (UC Berkeley), and Arthur Gervais (University College London)*

BlindHub: Bitcoin-Compatible Privacy-Preserving Payment Channel Hubs Supporting Variable Amounts ........ 2462
*Xianrui Qin (The University of Hong Kong), Shimin Pan (The University of Hong Kong), Arash Mirzaei (Monash University), Zhimei Sui (Monash University), Oguzhan Ersoy (Radboud University and Delft University of Technology), Amin Sakzad (Monash University), Muhammed Esgin (Monash University and CSIRO's Data61), Joseph K. Liu (Monash University), Jiangshan Yu (Monash University), and Tsz Hon Yuen (The University of Hong Kong)*

Optimistic Fast Confirmation While Tolerating Malicious Majority in Blockchains ........ 2481
*Ruomu Hou (National University of Singapore) and Haifeng Yu (National University of Singapore)*

Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts ........ 2499
*Kushal Babel (Cornell Tech), Philip Daian (Cornell Tech), Mahimna Kelkar (Cornell Tech), and Ari Juels (Cornell Tech)*

Tyr: Finding Consensus Failure Bugs in Blockchain System with Behaviour Divergent Model ........ 2517
*Yuanliang Chen (Tsinghua University), Fuchen Ma (Tsinghua University), Yuanhang Zhou (Tsinghua University), Yu Jiang (Tsinghua University), Ting Chen (University of Electronic Science and Technology of China), and Jiaguang Sun (Tsinghua University)*

Leaking Arbitrarily Many Secrets: Any-out-of-Many Proofs and Applications to RingCT Protocols ........ 2533
*Tianyu Zheng (The Hong Kong Polytechnic University), Shang Gao (The Hong Kong Polytechnic University), Yubo Song (Southeast University), and Bin Xiao (The Hong Kong Polytechnic University)*

## Session 9C: Malware and malicious sites

Could you clean up the Internet with a Pit of Tar? Investigating tarpit feasibility on Internet worms ........ 2551
*Harm Griffioen (Hasso Plattner Institute for Digital Engineering, University of Potsdam) and Christian Doerr (Hasso Plattner Institute for Digital Engineering, University of Potsdam)*

Beyond Phish: Toward Detecting Fraudulent e-Commerce Websites at Scale ........ 2566
*Marzieh Bitaab (Arizona State University), Haehyun Cho (Soongsil University), Adam Oest (PayPal, Inc.), Zhuoer Lyu (Arizona State University), Wei Wang (Palo Alto Networks), Jorij Abraham (Scam Adviser), Ruoyu Wang (Arizona State University), Tiffany Bao (Arizona State University), Yan Shoshitaishvili (Arizona State University), and Adam Doupé (Arizona State University)*

Limits of I/O Based Ransomware Detection: An Imitation Based Attack ..... 2584
*Chijin Zhou (Tsinghua University, China), Lihua Guo (Tsinghua University, China), Yiwei Hou (Tsinghua University, China), Zhenya Ma (Tsinghua University, China), Quan Zhang (Tsinghua University, China), Mingzhe Wang (Tsinghua University, China), Zhe Liu (Nanjing University of Aeronautics and Astronautics, China), and Yu Jiang (Tsinghua University, China)*

From Grim Reality to Practical Solution: Malware Classification in Real-World Noise ..... 2602
*Xian Wu (Northwestern University), Wenbo Guo (UC Berkeley), Jia Yan (Penn State), Baris Coskun (AWS), and Xinyu Xing (Northwestern University)*

SoK: History is a Vast Early Warning System: Auditing the Provenance of System Intrusions ..... 2620
*Muhammad Adil Inam (University of Illinois at Urbana-Champaign), Yinfang Chen (University of Illinois at Urbana-Champaign), Akul Goyal (University of Illinois at Urbana-Champaign), Jason Liu (University of Illinois at Urbana-Champaign), Jaron Mink (University of Illinois at Urbana-Champaign), Noor Michael (University of Illinois at Urbana-Champaign), Sneha Gaur (University of Illinois at Urbana-Champaign), Adam Bates (University of Illinois at Urbana-Champaign), and Wajih Ul Hassan (University of Virginia)*

Collaborative Ad Transparency: Promises and Limitations ..... 2639
*Eleni Gkiouzepi (Technical University of Berlin, Germany), Athanasios Andreou (Algorithmic Transparency Institute, USA), Oana Goga (CNRS, Inria, Institut Polytechnique de Paris, France), and Patrick Loiseau (Inria, FairPlay team, France)*

## Session 10A: Fuzzing

Toss a Fault to Your Witcher: Applying Grey-box Coverage-Guided Mutational Fuzzing to Detect SQL and Command Injection Vulnerabilities ..... 2658
*Erik Trickel (Arizona State University), Fabio Pagani (UC Santa Barbara), Chang Zhu (Arizona State University), Lukas Dresel (UC Santa Barbara), Giovanni Vigna (UC Santa Barbara), Christopher Kruegel (UC Santa Barbara), Ruoyu Wang (Arizona State University), Tiffany Bao (Arizona State University), Yan Shoshitaishvili (Arizona State University), and Adam Doupe (Arizona State University)*

UTOPIA: Automatic Generation of Fuzz Driver using Unit Tests ..... 2676
*Bokdeuk Jeong (Samsung Research, Republic of Korea), Joonun Jang (Samsung Research, Republic of Korea), Hayoon Yi (Samsung Research, Republic of Korea), Jiin Moon (Samsung Research, Republic of Korea), Junsik Kim (Samsung Research, Republic of Korea), Intae Jeon (Samsung Research, Republic of Korea), Taesoo Kim (Samsung Research, Republic of Korea; Georgia Institute of Technology, USA), WooChul Shim (Samsung Research, Republic of Korea), and Yong Ho Hwang (Samsung Research, Republic of Korea)*

SelectFuzz: Efficient Directed Fuzzing with Selective Path Exploration ..... 2693
*Changhua Luo (Chinese University of Hong Kong), Wei Meng (Chinese University of Hong Kong), and Penghui Li (Chinese University of Hong Kong)*

Finding Specification Blind Spots via Fuzz Testing .......... 2708
*Ru Ji (University of Waterloo) and Meng Xu (University of Waterloo)*

ODDFUZZ: Discovering Java Deserialization Vulnerabilities via Structure-Aware Directed Greybox Fuzzing .......... 2726
*Sicong Cao (Yangzhou University, China), Biao He (Ant Group, China), Xiaobing Sun (Yangzhou University, China), Yu Ouyang (Ant Group, China), Chao Zhang (Tsinghua University, China), Xiaoxue Wu (Yangzhou University, China), Ting Su (East China Normal University), Lili Bo (Yangzhou University, China), Bin Li (Yangzhou University, China), Chuanlei Ma (Ant Group, China), Jiajia Li (Ant Group, China), and Tao Wei (Ant Group, China)*

## Session 10B: Web security

The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web. 2744
*Jannis Rautenstrauch (CISPA Helmholtz Center for Information Security, Germany), Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany), and Ben Stock (CISPA Helmholtz Center for Information Security, Germany)*

WebSpec: Towards Machine-Checked Analysis of Browser Security Mechanisms .......... 2761
*Lorenzo Veronese (TU Wien), Benjamin Farinier (Univ Rennes, Inria, CNRS, IRISA), Pedro Bernardo (TU Wien), Mauro Tempesta (TU Wien), Marco Squarcina (TU Wien), and Matteo Maffei (TU Wien)*

Detection of Inconsistencies in Privacy Practices of Browser Extensions .......... 2780
*Duc Bui (University of Michigan, United States of America), Brian Tang (University of Michigan, United States of America), and Kang G. Shin (University of Michigan, United States of America)*

TeSec: Accurate Server-side Attack Investigation for Web Applications .......... 2799
*Ruihua Wang (KLISS, TNList, School of Software, Tsinghua University), Yihao Peng (KLISS, TNList, School of Software, Tsinghua University), Yilun Sun (KLISS, TNList, School of Software, Tsinghua University), Xuancheng Zhang (KLISS, TNList, School of Software, Tsinghua University), Hai Wan (KLISS, TNList, School of Software, Tsinghua University), and Xibin Zhao (KLISS, TNList, School of Software, Tsinghua University)*

RuleKeeper: GDPR-Aware Personal Data Compliance for Web Frameworks .......... 2817
*Mafalda Ferreira (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa), Tiago Brito (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa), José Fragoso Santos (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa), and Nuno Santos (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa)*

## Session 10C: Human factors 2

Characterizing Everyday Misuse of Smart Home Devices ........ 2835
*Phoebe Moh (University of Maryland, USA), Pubali Datta (University of Illinois Urbana-Champaign, USA), Noel Warford (University of Maryland, USA), Adam Bates (University of Illinois Urbana-Champaign, USA), Nathan Malkin (University of Maryland, USA), and Michelle Mazurek (University of Maryland, USA)*

"It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit ........ 2850
*Jingjie Li (University of Wisconsin-Madison, USA), Kaiwen Sun (University of Michigan, USA), Brittany Skye Huff (University of Wisconsin-Madison, USA), Anna Marie Bierley (University of Wisconsin-Madison, USA), Younghyun Kim (University of Wisconsin-Madison, USA), Florian Schaub (University of Michigan, USA), and Kassem Fawaz (University of Wisconsin-Madison, USA)*

User Perceptions and Experiences with Smart Home Updates ........ 2867
*Julie Haney (National Institute of Standards and Technology, USA) and Susanne Furman (National Institute of Standards and Technology, USA)*

Design and Evaluation of Inclusive Email Security Indicators for People with Visual Impairments ........ 2885
*Yaman Yu (University of Illinois at Urbana-Champaign, USA), Saidivya Ashok (University of Illinois at Urbana-Champaign / CMU, USA), Smirity Kaushi (University of Illinois at Urbana-Champaign, USA), Yang Wang (University of Illinois at Urbana-Champaign, USA), and Gang Wang (University of Illinois at Urbana-Champaign, USA)*

When and Why Do People Want Ad Targeting Explanations? Evidence from a Four-Week, Mixed-Methods Field Study ........ 2903
*Hao-Ping Lee (Carnegie Mellon University, USA), Jacob Logas (Georgia Institute of Technology, USA), Stephanie Yang (Georgia Institute of Technology, USA), Zhouyu Li (North Carolina State University, USA), Natã Barbosa (University of Illinois at Urbana-Champaign, USA), Yang Wang (University of Illinois at Urbana-Champaign, USA), and Sauvik Das (Carnegie Mellon University, USA)*

## Session 11A: Software isolation

SecureCells: A Secure Compartmentalized Architecture ........ 2921
*Atri Bhattacharyya (EPFL), Florian Hofhammer (EPFL), Yuanlong Li (EPFL), Siddharth Gupta (EPFL), Andres Sanchez (EPFL), Babak Falsafi (EPFL), and Mathias Payer (EPFL)*

WaVe: A Verifiably Secure WebAssembly Sandboxing Runtime ........ 2940
*Evan Johnson (UC San Diego, USA), Evan Laufer (Stanford, USA), Zijie Zhao (UIUC, USA), Dan Gohman (Fastly Labs, USA), Shravan Narayan (UC San Diego, USA), Stefan Savage (UC San Diego, USA), Deian Stefan (UC San Diego, USA), and Fraser Brown (Carnegie Mellon University, USA)*

uSWITCH: Fast Kernel Context Isolation with Implicit Context Switches .................................. 2956
*Dinglan Peng (Purdue University), Congyu Liu (Purdue University), Tapti Palit (Purdue University), Pedro Fonseca (Purdue University), Anjo Vahldiek-Oberwagner (Intel Labs), and Mona Vij (Intel Labs)*

Control Flow and Pointer Integrity Enforcement in a Secure Tagged Architecture ....................... 2974
*Ravi Theja Gollapudi (State University of New York at Binghamton), Gokturk Yuksek (State University of New York at Binghamton), David Demicco (State University of New York at Binghamton), Matthew Cole (State University of New York at Binghamton), Gaurav N Kothari (State University of New York at Binghamton), Rohit H Kulkarni (State University of New York at Binghamton), Xin Zhang (State University of New York at Binghamton), Kanad Ghose (State University of New York at Binghamton), Aravind Prakash (State University of New York at Binghamton), and Zerksis Umrigar (State University of New York at Binghamton)*

EC: Embedded Systems Compartmentalization via Intra-Kernel Isolation ................................. 2990
*Arslan Khan (Purdue University), Dongyan Xu (Purdue University), and Dave Tian (Purdue University)*

Low-Cost Privilege Separation with Compile Time Compartmentalization for Embedded Systems ...... 3008
*Arslan Khan (Purdue University), Dongyan Xu (Purdue University), and Dave Tian (Purdue University)*

## Session 11B: IoT security

One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices ....................... 3026
*Habiba Farrukh (Purdue University, USA), Muslum Ozgur Ozmen (Purdue University, USA), Faik Kerem Ors (Purdue University, USA), and Z. Berkay Celik (Purdue University, USA)*

Optimistic Access Control for the Smart Home ...................................................................... 3043
*Nathan Malkin (University of Maryland), Alan F. Luo (University of Maryland), Julio Poveda (University of Maryland), and Michelle L. Mazurek (University of Maryland)*

Protected or Porous: A Comparative Analysis of Threat Detection Capability of IoT Safeguards ................................................................................................................ 3061
*Anna Maria Mandalari (University College London, UK), Hamed Haddadi (Imperial College London, UK), Daniel J. Dubois (Northeastern University, US), and David Choffnes (Northeastern University, US)*

LazyTAP: On-Demand Data Minimization for Trigger-Action Applications .............................. 3079
*Mohammad M. Ahmadpanah (Chalmers University of Technology, Sweden), Daniel Hedin (Chalmers University of Technology and Mälardalen University, Sweden), and Andrei Sabelfeld (Chalmers University of Technology, Sweden)*

Blue's Clues: Practical Discovery of Non-Discoverable Bluetooth Devices ................................ 3098
*Tyler Tucker (University of Florida), Hunter Searle (University of Florida), Kevin Butler (University of Florida), and Patrick Traynor (University of Florida)*

DeHiREC: Detecting Hidden Voice Recorders via ADC Electromagnetic Radiation ..................... 3113
*Ruochen Zhou (Zhejiang University), Xiaoyu Ji (Zhejiang University), Chen Yan (Zhejiang University), Yi-Chao Chen (Shanghai Jiao Tong University; Microsoft Research Asia), Wenyuan Xu (Zhejiang University), and Chaohao Li (Zhejiang University)*

## Session 11C: Network security

IPvSeeYou: Exploiting Leaked Identifiers in IPv6 for Street-Level Geolocation ........................... 3129
*Erik Rye (University of Maryland) and Robert Beverly (CMAND)*

From 5G Sniffing to Harvesting Leakages of Privacy-Preserving Messengers ............................ 3146
*Norbert Ludant (Northeastern University, USA), Pieter Robyns (Hasselt University - tUL - EDM and Belgian Cyber Command, Belgium), and Guevara Noubir (Northeastern University, USA)*

Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects ................... 3162
*Xuewei Feng (Tsinghua University, China), Qi Li (Tsinghua University and Zhongguancun Lab, China), Kun Sun (George Mason University, USA), Yuxiang Yang (Tsinghua University), and Ke Xu (Tsinghua University and Zhongguancun Lab, China)*

Mew: Enabling Large-Scale and Dynamic Link-Flooding Defenses on Programmable Switches .... 3178
*Huancheng Zhou (Texas A&M University), Sungmin Hong (Texas A&M University), Yangyang Liu (The Hong Kong Polytechnic University), Xiapu Luo (The Hong Kong Polytechnic University), Weichao Li (Peng Cheng Laboratory), and Guofei Gu (Texas A&M University)*

PCspooF: Compromising the Safety of Time-Triggered Ethernet .............................................. 3193
*Andrew Loveless (University of Michigan; NASA Johnson Space Center), Linh Thi Xuan Phan (University of Pennsylvania), Ronald Dreslinski (University of Michigan), and Baris Kasikci (University of Michigan)*

BLEDiff : Scalable and Property-Agnostic Noncompliance Checking for BLE Implementations .... 3209
*Imtiaz Karim (Purdue University), Abdullah Al Ishtiaq (Pennsylvania State University), Syed Rafiul Hussain (Pennsylvania State University), and Elisa Bertino (Purdue University)*

## Session 12A: Bug finding

VIDEZZO: Dependency-aware Virtual Device Fuzzing .......................................................... 3228
*Qiang Liu (Zhejiang University, China; EPFL, Switzerland), Flavio Toffalini (EPFL, Switzerland), Yajin Zhou (Zhejiang University, China), and Mathias Payer (EPFL, Switzerland)*

DEVFUZZ: Automatic Device Model-Guided Device Driver Fuzzing ....................................... 3246
*Yilun Wu (Stony Brook University), Tong Zhang (Samsung Electronics), Changhee Jung (Purdue University), and Dongyoon Lee (Stony Brook University)*

SyzDescribe: Principled, Automated, Static Generation of Syscall Descriptions for Kernel Drivers ........ 3262
*Yu Hao (University of California, Riverside), Guoren Li (University of California, Riverside), Xiaochen Zou (University of California, Riverside), Weiteng Chen (University of California, Riverside), Shitong Zhu (University of California, Riverside), Zhiyun Qian (University of California, Riverside), and Ardalan Amiri Sani (University of California, Irvine)*

QueryX: Symbolic Query on Decompiled Code for Finding Bugs in COTS Binaries ........ 3279
*HyungSeok Han (Theori Inc., KAIST), JeongOh Kyea (Theori Inc.), Yonghwi Jin (Theori Inc.), Jinoh Kang (Theori Inc.), Brian Pak (Theori Inc.), and Insu Yun (KAIST)*

PyFET: Forensically Equivalent Transformation for Python Binary Decompilation ........ 3296
*Ali Ahad (University of Virginia, USA), Chijung Jung (University of Virginia, USA), Ammar Askar (Georgia Institute of Technology, USA), Doowon Kim (University of Tennessee, USA), Taesoo Kim (Georgia Institute of Technology, USA), and Yonghwi Kwon (University of Virginia, USA)*

## Session 12B: Election and device recycling security

Adaptive Risk-Limiting Comparison Audits ........ 3314
*Abigail Harrison (University of Connecticut), Benjamin Fuller (University of Connecticut), and Alexander Russell (University of Connecticut)*

Blue Is the New Black (Market): Privacy Leaks and Re-Victimization from Police-Auctioned Cellphones ........ 3332
*Richard Roberts (University of Maryland, USA), Julio Poveda (University of Maryland, USA), Raley Roberts (University of Maryland, USA), and Dave Levin (University of Maryland, USA)*

No Privacy in the Electronics Repair Industry ........ 3347
*Jason Ceci (University of Guelph, Canada), Jonah Stegman (University of Guelph, Canada), and Hassan Khan (University of Guelph, Canada)*

How IoT Re-using Threatens Your Sensitive Data: Exploring the User-Data Disposal in Used IoT Devices ........ 3365
*Peiyu Liu (Zhejiang University, China), Shouling Ji (Zhejiang University, China), Lirong Fu (Zhejiang University, China), Kangjie Lu (University of Minnesota, USA), Xuhong Zhang (Zhejiang University, China), Jingchang Qin (Zhejiang University, China), Wenhai Wang (Zhejiang University, China), and Wenzhi Chen (Zhejiang University, China)*

## Session 12C: Physical channels 2

Privacy Leakage via Unrestricted Motion-Position Sensors in the Age of Virtual Reality: A Study of Snooping Typed Input on Virtual Keyboards ........ 3382
*Yi Wu (University of Tennessee, Knoxville, USA), Cong Shi (New Jersey Institute of Technology, USA), Tianfang Zhang (Rutgers University, USA), Payton Walker (Texas A&M University, College Station, USA), Jian Liu (University of Tennessee, Knoxville, USA), Nitesh Saxena (Texas A&M University, College Station, USA), and Yingying Chen (Rutgers University, USA)*

Uncovering User Interactions on Smartphones via Contactless Wireless Charging Side Channels ........ 3399
*Tao Ni (City University of Hong Kong), Xiaokuan Zhang (George Mason University), Chaoshun Zuo (The Ohio State University), Jianfeng Li (The Hong Kong Polytechnic University), Zhenyu Yan (The Chinese University of Hong Kong), Wubing Wang (DBAPPSecurity Co., Ltd), Weitao Xu (City University of Hong Kong), Xiapu Luo (The Hong Kong Polytechnic University), and Qingchuan Zhao (City University of Hong Kong)*

MagBackdoor: Beware of Your Loudspeaker as a Backdoor for Magnetic Injection Attacks ........ 3416
*Tiantian Liu (Zhejiang University, China), Feng Lin (Zhejiang University, China), Zhangsen Wang (Zhejiang University, China), Chao Wang (Zhejiang University, China), Zhongjie Ba (Zhejiang University, China), Li Lu (Zhejiang University, China), Wenyao Xu (University at Buffalo, USA), and Kui Ren (Zhejiang University, China)*

Private Eye: On the Limits of Textual Screen Peeking via Eyeglass Reflections in Video Conferencing ........ 3432
*Yan Long (University of Michigan, USA), Chen Yan (Zhejiang University, China), Shilin Xiao (Zhejiang University, China), Shivan Prasad (University of Michigan, USA), Wenyuan Xu (Zhejiang University, China), and Kevin Fu (University of Michigan, USA)*

Low-effort VR Headset User Authentication Using Head-reverberated Sounds with Replay Resistance ........ 3450
*Ruxin Wang (Louisiana State University), Long Huang (Louisiana State University), and Chen Wang (Louisiana State University)*

**Author Index**