

2024 Annual Computer Security Applications Conference (ACSAC 2024)

**Honolulu, Hawaii, USA
9-13 December 2024**

Pages 1-635



**IEEE Catalog Number: CFP24393-POD
ISBN: 979-8-3315-2089-2**

**Copyright © 2024 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:	CFP24393-POD
ISBN (Print-On-Demand):	979-8-3315-2089-2
ISBN (Online):	979-8-3315-2088-5
ISSN:	1063-9527

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

2024 Annual Computer Security Applications Conference (ACSAC) **ACSAC 2024**

Table of Contents

Message from the Conference Chairs	xvii
Message from the Program Chairs	xix
Message from the Artifacts Evaluation Chairs	xxi
Organizing Committee	xxii
Steering Committee	xxiv
Program Committee	xxv
Reviewers	xxix
Artifacts Evaluation Committee	xxx
Cybersecurity Artifacts Competition and Impact Award Committee	xxxii
Test of Time Awards Committee	xxxiii
ACSAC Capture-the-Flag Organizing Committee	xxxiv
Message from the Sponsor: Applied Computer Security Associates (ACSA)	xxxv
ACSA Members	xxxvii

Generative AI (for) Security

Enhancing Database Encryption: Adaptive Measures for Digital Assets Against LLMs-Based Reverse Engineering	1
<i>Kerou Zhou (Tsinghua University, China), Jiakang Qiu (Tsinghua University, China), Yuehua Wang (Academy of Military Science, China), and Xiaojun Ye (Tsinghua University, China)</i>	
SECURE: Benchmarking Large Language Models for Cybersecurity	15
<i>Dipkamal Bhusal (Rochester Institute of Technology, USA), Md Tanvirul Alam (Rochester Institute of Technology, USA), Le Nguyen (Rochester Institute of Technology, USA), Ashim Mahara (RIT, USA), Zachary Lightcap (RIT, USA), Rodney Frazier (RIT, USA), Romy Fieblinger (RIT, USA), Grace Long Torales (RIT, USA), Benjamin A. Blakely (Argonne National Lab, USA), and Nidhi Rastogi (Rochester Institute of Technology (RIT), USA)</i>	
Not All Tokens Are Equal: Membership Inference Attacks Against Fine-Tuned Language Models ...	31
<i>Changtian Song (Wuhan University of Technology, China), Dongdong Zhao (Wuhan University of Technology, China), and Jianwen Xiang (Wuhan University of Technology, China)</i>	

Stealing Watermarks of Large Language Models via Mixed Integer Programming	46
<i>Zhaoxi Zhang (University of Technology Sydney, Australia), Xiaomei Zhang (Griffith University, Australia), Yanjun Zhang (University of Technology Sydney, Australia), Leo Yu Zhang (Griffith University, Australia), Chao Chen (Royal Melbourne Institute of Technology, Australia), Shengshan Hu (Huazhong University of Science and Technology, Australia), Asif Gill (University of Technology Sydney, Australia), and Shirui Pan (Griffith University, Australia)</i>	
Towards a Taxonomy of Challenges in Security Control Implementation	61
<i>Md Rayhanur Rahman (North Carolina State University), Brandon Wroblewski (North Carolina State University), Mahzabin Tamanna (North Carolina State University), Imranur Rahman (North Carolina State University), Andrew Anufryienak (University of North Carolina at Charlotte), and Laurie Williams (North Carolina State University)</i>	

Virtualization and Cloud Security

CubeVisor: A Multi-Realm Architecture Design for Running VM with ARM CCA	76
<i>Jiayun Chen (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Qihang Zhou (Chinese Academy of Sciences, China), Xiaolong Yan (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Nan Jiang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xiaoqi Jia (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and WeiJuan Zhang (Chinese Academy of Sciences, China)</i>	
ConProv: A Container-Aware Provenance System for Attack Investigation	89
<i>Qiqing Deng (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yanqiang Zhang (China Mobile Communications Corporation, China), Zhen Xu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Qian Tan (Chinese Academy of Sciences, China), and Yan Zhang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	
Confidential Computing with Heterogeneous Devices at Cloud-Scale	102
<i>Aritra Dhar (Huawei Zurich Research Center), Supraja Sridhara (ETH Zürich), Shweta Shinde (ETH Zürich), Srdjan Capkun (ETH Zürich), and Renzo Andri (Huawei Zurich Research Center)</i>	
Hypervisor Dissociative Execution: Programming Guests for Monitoring, Management, and Security	117
<i>Andrew Fasano (MIT Lincoln Laboratory, USA), Zak Estrada (MIT Lincoln Laboratory, USA), Tim Leek (MIT Lincoln Laboratory, USA), and William Robertson (Northeastern University, USA)</i>	
T-Edge: Trusted Heterogeneous Edge Computing	131
<i>Jiamin Shen (National University of Singapore), Yao Chen (National University of Singapore), Weng-Fai Wong (National University of Singapore), and Ee-Chien Chang (National University of Singapore)</i>	

Web Security and Privacy

Web-Armour: Mitigating Reconnaissance and Vulnerability Scanning with Scan-Impeding Delays in Web Deployments	144
<i>Yousif Dafalla (University of Kansas, USA), Dalton A. Brucker-Hahn (Sandia National Laboratories, USA), Drew Davidson (University of Kansas, USA), and Alexandru G. Bardas (University of Kansas, USA)</i>	
Harnessing Multiplicity: Granular Browser Extension Fingerprinting through User Configurations	161
<i>Konstantinos Solomos (University of Illinois Chicago, USA), Nick Nikiforakis (Stony Brook University, USA), and Jason Polakis (University of Illinois Chicago, USA)</i>	
Ready or Not, Here I Come: Characterizing the Security of Prematurely-Public Web Applications	175
<i>Brian Kondracki (Stony Brook University), Michael Ferdman (Stony Brook University), and Nick Nikiforakis (Stony Brook University)</i>	
You Only Perturb Once: Bypassing (Robust) Ad-Blockers using Universal Adversarial Perturbations	190
<i>Dongwon Shin (KAIST), Suyoung Lee (KAIST), Sanghyun Hong (Oregon State University), and Soel Son (KAIST)</i>	
A Longitudinal Analysis of Corporate Data Portability Practices Across Industries	207
<i>Emmanuel Syrmoudis (Technical University of Munich, Germany), Stefan A. Mager (Independent Researcher, Germany), and Jens Grossklags (Technical University of Munich, Germany)</i>	

Cyber-Physical Systems Security

Assault and Battery: Evaluating the Security of Power Conversion Systems Against Electromagnetic Injection Attacks	224
<i>Marcell Szakály (University of Oxford, United Kingdom), Sebastian Köhler (University of Oxford, United Kingdom), Martin Strohmeier (armasuisse, Switzerland), and Ivan Martinovic (University of Oxford, United Kingdom)</i>	
A Fly on the Wall - Exploiting Acoustic Side-Channels in Differential Pressure Sensors	240
<i>Yonatan Gizachew Achamyelch (University of California, USA), Mohamad Habib Fakih (University of California, USA), Gabriel Garcia (University of California, USA), Anomadarshi Barua (George Mason University, USA), and Mohammad Abdullah Al Faruque (University of California, USA)</i>	
TRACES: TEE-Based Runtime Auditing for Commodity Embedded Systems	257
<i>Adam Caulfield (Rochester Institute of Technology, USA), Antonio Joia Neto (Rochester Institute of Technology, USA), Norrathep Rattanavipanon (Prince of Songkla University, Thailand), and Ivan De Oliveira Nunes (Rochester Institute of Technology, USA)</i>	

BioSaFe: Bioprinting Security Framework for Detecting Sabotage Attacks on Printability and Cell Viability	271
<i>Muhammad Ahsan (Virginia Commonwealth University (VCU), USA), Eunice Pak (Virginia Commonwealth University (VCU), USA), Kate Jackson (Virginia Commonwealth University (VCU), USA), Muhammad Haris Rais (Virginia State University (VSU), USA), Barry Najarro-Blancas (Virginia Commonwealth University (VCU), USA), Nastassja Lewinski (Virginia Commonwealth University (VCU), USA), and Irfan Ahmed (Virginia Commonwealth University (VCU), USA)</i>	

Passwords and Authentication

Leaky Autofill: An Empirical Study on the Privacy Threat of Password Managers' Autofill Functionality	288
<i>Yanduo Fu (Nankai University, China) and Ding Wang (Nankai University, China)</i>	
Passwords To-Go: Investigating Multifaceted Challenges for Password Managers in the Android Ecosystem	304
<i>Nicolas Huaman (Leibniz University Hannover), Marten Oltrogge (CISPA Helmholtz Center for Information Security), Sabrina Klivan (CISPA Helmholtz Center for Information Security), Yannick Evers (Leibniz University Hannover), and Sascha Fahl (CISPA Helmholtz Center for Information Security)</i>	
Single Sign-On Privacy: We Still Know What You Did Last Summer	321
<i>Maximilian Westers (Heilbronn University of Applied Sciences), Andreas Mayer (Heilbronn University of Applied Sciences), and Louis Jannett (Ruhr University Bochum)</i>	
FreeAuth: Privacy-Preserving Email Ownership Authentication with Verification-Email-Free	336
<i>Yijia Fang (Beihang University, China), Bingyu Li (Beihang University, China), Jiale Xiao (Beihang University, China), Bo Qin (Renmin University of China, China), Zhijintong Zhang (Beihang University, China), and Qianhong Wu (Beihang University, China)</i>	
Securing PUFs via a Predictive Adversarial Machine Learning System by Modeling of Attackers	353
<i>Mieszko Ferens (Aalborg University, Denmark), Edlira Dushku (Aalborg University, Denmark), Shreyas Srinivasa (Terma A.S., Denmark), and Sokol Kosta (Aalborg University, Denmark)</i>	

Microarchitectural Attacks and Side-Channels

No Leakage Without State Change: Repurposing Configurable CPU Exceptions to Prevent Microarchitectural Attacks	366
<i>Daniel Weber (CISPA Helmholtz Center for Information Security), Leonard Niemann (usd AG), Lukas Gerlach (CISPA Helmholtz Center for Information Security), Jan Reineke (Saarland University), and Michael Schwarz (CISPA Helmholtz Center for Information Security)</i>	
Faking Deduplication to Prevent Timing Side-Channel Attacks on Memory Deduplication	380
<i>Jens Lindemann (University of Hamburg, Germany)</i>	

R+R: Demystifying ML-Assisted Side-Channel Analysis Framework: A Case of Image Reconstruction	393
<i>Zhiyuan Zhang (The University of Melbourne, Australia), Zhenzhi Lai (The University of Melbourne, Australia), and Udaya Parampalli (The University of Melbourne, Australia)</i>	
Reading It Like an Open Book: Single-Trace Blind Side-Channel Attacks on Garbled Circuit Frameworks	410
<i>Sirui Shen (Centrum Wiskunde & Informatica, The Netherlands) and Chenglu Jin (Centrum Wiskunde & Informatica, The Netherlands)</i>	
SecurityHub: Electromagnetic Fingerprinting USB Peripherals using Backscatter-Assisted Commodity Hardware	425
<i>Si Liao (ShanghaiTech University), Huangxun Chen (HKUST (GZ)), and Zhice Yang (ShanghaiTech University)</i>	

Cryptocurrency and Payment Security

Breaking the Privacy Barrier: On the Feasibility of Reorganization Attacks on Ethereum Private Transactions	439
<i>Mengya Zhang (The Ohio State University, USA), Xingyu Lyu (University of Massachusetts, USA), Jianyu Niu (Southern University of Science and Technology, China), Xiaokuan Zhang (George Mason University, USA), Yinqian Zhang (Southern University of Science and Technology, China), and Zhiqiang Lin (The Ohio State University, USA)</i>	
RouTEE: Secure, Scalable, and Efficient Off-Chain Payments using Trusted Execution Environments	456
<i>Junmo Lee (Seoul National University, Republic of Korea), Seongjun Kim (Seoul National University, Republic of Korea), Sanghyeon Park (Seoul National University, Republic of Korea), and Soo-Mook Moon (Seoul National University, Republic of Korea)</i>	
Practical Light Clients for Committee-Based Blockchains	473
<i>Frederik Armknecht (Universität Mannheim), Ghassan Karame (Ruhr-Universität Bochum), Malcom Mohamed (Ruhr-Universität Bochum), and Christiane Weis (NEC Laboratories Europe)</i>	
JANUS: Enhancing Asynchronous Common Subset with Trusted Hardware	488
<i>Liangrong Zhao (Monash University), Hans Schmiedel (Monash University), Qin Wang (CSIRO Data61, Australia), and Jiangshan Yu (University of Sydney)</i>	
Verifying Loot-box Probability Without Source-Code Disclosure	505
<i>Jing-Jie Wang (National Taiwan University), An-Jie Li (National Taiwan University), Ting-Yu Fang (National Taiwan University), and Hsu-Chun Hsiao (National Taiwan University)</i>	

System Security

I'll Be There for You! Perpetual Availability in the A ⁸ MVX System	520
<i>André Rösti (University of California, USA), Stijn Volckaert (KU Leuven, Belgium), Michael Franz (University of California, USA), and Alexios Voulimeneas (TU Delft, The Netherlands)</i>	

SIDECAR: Leveraging Debugging Extensions in Commodity Processors to Secure Software	534
<i>Konstantinos Kleftogiorgos (Stevens Institute of Technology, USA), Patrick Zielinski (Stevens Institute of Technology, USA), Shan Huang (Stevens Institute of Technology, USA), Jun Xu (University of Utah, USA), and Georgios Portokalidis (IMDEA Software Institute, Spain)</i>	
Rust for Linux: Understanding the Security Impact of Rust in the Linux Kernel	548
<i>Zhaofeng Li (University of Utah), Vikram Narayanan (Palo Alto Networks), Xiangdong Chen (University of Utah), Jerry Zhang (University of Utah), and Anton Burtsev (University of Utah)</i>	
SpecCFA: Enhancing Control Flow Attestation/Auditing via Application-Aware Sub-Path Speculation	563
<i>Adam Caulfield (Rochester Institute of Technology, USA), Liam Tyler (Rochester Institute of Technology, USA), and Ivan De Oliveira Nunes (Rochester Institute of Technology, USA)</i>	
SECvma: Virtualization-Based Linux Kernel Protection for Arm	579
<i>Teh Beng Yen (National Taiwan University), Joey Li (National Taiwan University), and Shih-Wei Li (National Taiwan University)</i>	

IoT and Smart Home Security

WiShield: Fine-Grained Countermeasure Against Malicious Wi-Fi Sensing in Smart Home	593
<i>Yihui Yan (ShanghaiTech University, China) and Zhice Yang (ShanghaiTech University, China)</i>	
AirBugCatcher: Automated Wireless Reproduction of IoT Bugs	607
<i>Guoqiang Hua (SUTD, Singapore), Matheus E. Garbelini (SUTD, Singapore), and Sudipta Chattopadhyay (SUTD, Singapore)</i>	
VaktBLE: A Benevolent Man-in-the-Middle Bridge to Guard against Malevolent BLE Connections.	621
<i>Geovani Benita (SUTD), Leonardo Sestrem (SUTD), Matheus E. Garbelini (SUTD), Sudipta Chattopadhyay (SUTD), Sumei Sun (A*STAR), and Ernest Kurniawan (A*STAR)</i>	
BlueScream: Screaming Channels on Bluetooth Low Energy	636
<i>Pierre Ayoub (EURECOM, France), Romain Cayre (EURECOM, France), Aurélien Francillon (EURECOM, France), and Clémentine Maurice (Univ. Lille, France)</i>	
Eunomia: A Real-Time Privacy Compliance Firewall for Alexa Skills	650
<i>Javaria Ahmad (University of Central Missouri, USA), Fengjun Li (The University of Kansas, USA), Razvan Beuran (Japan Advanced Institute of Science and Technology, Japan), and Bo Luo (The University of Kansas, USA)</i>	

Privacy Enhancing Technologies

R+R: Towards Reliable and Generalizable Differentially Private Machine Learning	666
<i>Wenxuan Bao (University of Florida, USA) and Vincent Bindschaedler (University of Florida, USA)</i>	

Privacy-Preserving Verifiable Neural Network Inference Service	683
<i>Arman Riasi (Virginia Tech), Jorge Guajardo (Robert Bosch LLC — RTC), and Thang Hoang (Virginia Tech)</i>	
R+R: Revisiting Graph Matching Attacks on Privacy-Preserving Record Linkage	699
<i>Jochen Schäfer (University of Mannheim, Germany), Frederik Armknecht (University of Mannheim, Germany), and Youzhe Heng (University of Mannheim, Germany)</i>	
FA-SEAL: Forensically Analyzable Symmetric Encryption for Audit Logs	716
<i>Basanta Chaulagain (University of Georgia, USA) and Kyu Hyung Lee (University of Georgia, USA)</i>	
FLUENT: A Tool for Efficient Mixed-Protocol Semi-Private Function Evaluation	733
<i>Daniel Günther (Technical University of Darmstadt, Germany), Joachim Schmidt (Technical University of Darmstadt, Germany), Thomas Schneider (Technical University of Darmstadt, Germany), and Hossein Yalame (Technical University of Darmstadt, Germany)</i>	

Machine Learning Security I: Federated Learning

FedCAP: Robust Federated Learning via Customized Aggregation and Personalization	747
<i>Youpeng Li (University of Texas at Dallas, USA), Xinda Wang (University of Texas at Dallas, USA), Fuxun Yu (Microsoft, USA), Lichao Sun (Lehigh University, USA), Wenbin Zhang (Florida International University, USA), and Xuyu Wang (Florida International University, USA)</i>	
Link Inference Attacks in Vertical Federated Graph Learning	761
<i>Oualid Zari (EURECOM, France), Chuan Xu (Univ. Côte d’Azur, France), Javier Parra-Arnau (Universitat Politècnica de Catalunya, Spain), Ayşe Ünsal (EURECOM, France), and Melek Önen (EURECOM, France)</i>	
Efficient Secure Aggregation for Privacy-Preserving Federated Machine Learning	778
<i>Rouzbeh Behnia (University of South Florida), Arman Riasi (Virginia Tech), Reza Ebrahimi (University of South Florida), Sherman S. M. Chow (The Chinese University of Hong Kong), Balaji Padmanabhan (University of Maryland, College Park), and Thang Hoang (Virginia Tech)</i>	
Adversarially Guided Stateful Defense Against Backdoor Attacks in Federated Deep Learning	794
<i>Hassan Ali (UNSW Sydney), Surya Nepal (Data61 CSIRO), Salil S. Kanhere (Data61 CSIRO), and Sanjay Jha (Data61 CSIRO)</i>	

Lightweight Secure Aggregation for Personalized Federated Learning with Backdoor Resistance	810
<i>Tingyu Fan (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; University of Chinese Academy of Sciences, China), Xiaojun Chen (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; University of Chinese Academy of Sciences, China), Ye Dong (Singapore University of Technology and Design, Singapore), Xudong Chen (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Yuexin Xuan (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; University of Chinese Academy of Sciences, China), and Weizhan Jing (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; University of Chinese Academy of Sciences, China)</i>	

Malware and Intrusion Detection

DEEPCAPA: Identifying Malicious Capabilities in Windows Malware	826
<i>Saastha Vasan (University of California, Santa Barbara), Hojjat Aghakhani (University of California, Santa Barbara), Stefano Ortolani (Broadcom), Roman Vasilenko (Google), Ilya Grishchenko (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara), and Giovanni Vigna (University of California, Santa Barbara)</i>	
R+R: Matrioska: A User-Centric Defense Against Virtualization-Based Repackaging Malware on Android	843
<i>Simone Zerbini (University of Padua, Italy), Samuele Doria (University of Padua, Italy), Primal Wijesekera (International Computer Science Institute, USA), Serge Egelman (University of California Berkeley, USA), and Eleonora Losiuk (University of Padua, Italy)</i>	
IoC Stalker: Early Detection of Indicators of Compromise	857
<i>Mariella Mischinger (IMDEA Networks Institute and Universidad Carlos III de Madrid, Spain), Sergio Pastrana (Universidad Carlos III de Madrid, Spain), and Guillermo Suarez-Tangil (IMDEA Networks Institute, Spain)</i>	
Madeline: Continuous and Low-Cost Monitoring with Graph-Free Representations to Combat Cyber Threats	874
<i>Wenjia Song (Virginia Tech), Hailun Ding (Rutgers University), Na Meng (Virginia Tech), Peng Gao (Virginia Tech), and Danfeng Yao (Virginia Tech)</i>	
A Security Alert Investigation Tool Supporting Tier 1 Analysts in Contextualizing and Understanding Network Security Events	890
<i>Leon Kersten (Eindhoven University of Technology), Santiago Darré (Eindhoven University of Technology), Tom Mulders (Eindhoven University of Technology), Emmanuele Zambon (Eindhoven University of Technology), Marco Caselli (Siemens), Chris Snijders (Eindhoven University of Technology), and Luca Allodi (Eindhoven University of Technology)</i>	

Machine Learning Security II: Backdoors & Attacks

Evil from Within: Machine Learning Backdoors Through Dormant Hardware Trojans	906
<i>Alexander Warnecke (Berlin Institute for the Foundations of Learning and Data (BIFOLD); Technische Universität Berlin), Julian Speith (Max Planck Institute for Security and Privacy (MPI-SP); Max Planck Institute for Security and Privacy (MPI-SP)), Jan-Niklas Möller (Max Planck Institute for Security and Privacy (MPI-SP)), Konrad Rieck (Berlin Institute for the Foundations of Learning and Data (BIFOLD); Technische Universität Berlin), and Christof Paar (Max Planck Institute for Security and Privacy (MPI-SP))</i>	
Exploring Inherent Backdoors in Deep Learning Models	923
<i>Guanhong Tao (University of Utah; Purdue University), Siyuan Cheng (Purdue University), Zhenting Wang (Rutgers University), Shiqing Ma (University of Massachusetts Amherst), Shengwei An (Purdue University), Yingqi Liu (Microsoft), Guangyu Shen (Purdue University), Zhuo Zhang (Purdue University), Yunshu Mao (Purdue University), and Xiangyu Zhang (Purdue University)</i>	
On the Credibility of Backdoor Attacks Against Object Detectors in the Physical World	940
<i>Bao Gia Doan (University of Adelaide, Australia), Dang Quang Nguyen (University of Adelaide, Australia), Callum Lindquist (University of Adelaide, Australia), Paul Montague (Defence Science and Technology Group, Australia), Tamas Abraham (Defence Science and Technology Group, Australia), Olivier De Vel (CSIRO, Australia), Seyit Camtepe (CSIRO, Australia), Salil S. Kanhere (University of New South Wales, Australia), Ehsan Abbasnejad (University of Adelaide, Australia), and Damith C. Ranasinghe (University of Adelaide, Australia)</i>	
Physical ID-Transfer Attacks against Multi-Object Tracking via Adversarial Trajectory	957
<i>Chenyi Wang (University of Arizona), Yanmao Man (HERE Technologies), Raymond Muller (Purdue University), Ming Li (University of Arizona), Z. Berkay Celik (Purdue University), Ryan Gerdes (Virginia Tech), and Jonathan Petit (Qualcomm)</i>	
Model-Manipulation Attacks Against Black-Box Explanations	974
<i>Achyut Hegde (Karlsruhe Institute of Technology, Germany), Maximilian Noppel (Karlsruhe Institute of Technology, Germany), and Christian Wressnegger (Karlsruhe Institute of Technology, Germany)</i>	

(Autonomous) Vehicle Security

Moiré Injection Attack (MIA): Compromising Autonomous Vehicle Safety via Exploiting Camera's Color Filter Array (CFA) to Inject Hidden Traffic Sign	988
<i>Qi Xia (The University of Texas at San Antonio, USA) and Qian Chen (The University of Texas at San Antonio, USA)</i>	
Leveraging Intensity as a New Feature to Detect Physical Adversarial Attacks Against LiDARs	1002
<i>Yeji Park (Korea University, Republic of Korea), Hyunsu Cho (Korea University, Republic of Korea), Dong Hoon Lee (Korea University, Republic of Korea), and Wonsuk Choi (Korea University, Republic of Korea)</i>	

VIMU: Effective Physics-Based Realtime Detection and Recovery against Stealthy Attacks on UAVs	1015
<i>Yunbo Wang (Xidian University, China), Cong Sun (Xidian University, China), Qiaosen Liu (Xidian University, China), Bingnan Su (Xidian University, China), Zongxu Zhang (Xidian University, China), Michael Norris (The Pennsylvania State University, USA), Gang Tan (The Pennsylvania State University, USA), and Jianfeng Ma (Xidian University, China)</i>	
Assessing UAV Sensor Spoofing: More Than A GNSS Problem	1032
<i>Bailey Srimoungchanh (The University of Kansas), J. Garrett Morris (The University of Iowa), and Drew Davidson (The University of Kansas)</i>	

Application Security

R+R: Security Vulnerability Dataset Quality is Critical	1047
<i>Anurag Swarnim Yadav (University of Florida, USA) and Joseph N. Wilson (University of Florida, USA)</i>	
BinHunter: A Fine-Grained Graph Representation for Localizing Vulnerabilities in Binary Executables	1062
<i>Sima Arasteh (University of Southern California, CA), Jelena Mirkovic (University of Southern California, CA), Mukund Raghothaman (University of Southern California, CA), and Christophe Hauser (Dartmouth College, NH)</i>	
CryptoPyt: Unraveling Python Cryptographic APIs Misuse with Precise Static Taint Analysis	1075
<i>Xiangxin Guo (University of Science and Technology of China, China), Shijie Jia (Institute of Information Engineering, China), Jingqiang Lin (University of Science and Technology of China, China), Yuan Ma (Institute of Information Engineering, China), Fangyu Zheng (University of Chinese Academy of Sciences, China), Guangzheng Li (University of Science and Technology of China, China), Bowen Xu (Ningbo University, China), Yueqiang Cheng (NIO, China), and Kailiang Ji (NIO, China)</i>	
R+R: A Systematic Study of Cryptographic Function Identification Approaches in Binaries	1092
<i>Yongming Fan (Purdue University), Priyam Biswas (Intel), and Christina Garman (Purdue University)</i>	
Manifest Problems: Analyzing Code Transparency for Android Application Bundles	1109
<i>Florian Draschbacher (Graz University of Technology, Austria) and Lukas Maar (Graz University of Technology, Austria)</i>	

Network Security

I Can Show You the World (of Censorship): Extracting Insights from Censorship Measurement Data using Statistical Techniques	1123
<i>Anna Crowder (University of Florida), Daniel Olszewski (University of Florida), Patrick Traynor (University of Florida), and Kevin R. B. Butler (University of Florida)</i>	

Dissecting Open Edge Computing Platforms: Ecosystem, Usage, and Security Risks	1139
<i>Yu Bi (University of Science and Technology of China), Mingshuo Yang (Shandong University), Yong Fang (University of Science and Technology of China), Xianghang Mi (University of Science and Technology of China), Shangqing Guo (Shandong University; Shandong Key Laboratory of Artificial Intelligence Security), Shujun Tang (Qi An Xin Technology Research Institute), and Haixin Duan (Qi An Xin Technology Research Institute; Tsinghua University)</i>	
Assessing the Silent Frontlines: Exploring the Impact of DDoS Hacktivism in the Russo-Ukrainian War	1156
<i>Yagiz Yilmaz (Sabanci University, Turkey), Orcun Cetin (Sabanci University, Turkey), Omer Said Ozturk (Sabanci University, Turkey), Emre Ekmekcioglu (Sabanci University, Turkey), Budi Arief (University of Kent, UK), and Julio Hernandez-Castro (Universidad Politécnica de Madrid, Spain)</i>	
Robust Device Authentication in Multi-Node Networks: ML-Assisted Hybrid PLA Exploiting Hardware Impairments	1172
<i>Ildi Alla (Inria Lille-Nord Europe, France), Selma Yahia (Inria Lille-Nord Europe, France), Valeria Loscri (Inria Lille-Nord Europe, France), and Hossien Eldeeb (University of Cambridge, UK)</i>	
CloudCover: Enforcement of Multi-Hop Network Connections in Microservice Deployments	1186
<i>Dalton A. Brucker-Hahn (Sandia National Laboratories, USA), Wang Feng (University of North Texas, USA), Shanchao Li (University of North Texas, USA), Matthew Petillo (University of Kansas, USA), Alexandru G. Bardas (University of Kansas, USA), Drew Davidson (University of Kansas, USA), and Yuede Ji (University of Texas at Arlington, USA)</i>	

Machine Learning Security III: Potpourri

TILE: Input Structure Optimization for Neural Networks to Accelerate Secure Inference	1203
<i>Yizhou Feng (Old Dominion University, USA), Qiao Zhang (Chongqing University, China), Yifei Cai (Old Dominion University, USA), Hongyi Wu (University of Arizona, USA), and Chunsheng Xin (Old Dominion University, USA)</i>	
R+R: Understanding Hyperparameter Effects in DP-SGD	1217
<i>Felix Morsbach (Karlsruhe Institute of Technology, Germany), Jan Reubold (Karlsruhe Institute of Technology, Germany), and Thorsten Strufe (Karlsruhe Institute of Technology, Germany)</i>	
CIGA: Detecting Adversarial Samples via Critical Inference Graph Analysis	1231
<i>Fei Zhang (National University of Defense Technology, China; Key Laboratory of Advanced Microprocessor Chips and Systems, China), Zhe Li (National University of Defense Technology, China; Key Laboratory of Advanced Microprocessor Chips and Systems, China), Yahang Hu (National University of Defense Technology, China; Key Laboratory of Advanced Microprocessor Chips and Systems, China), and Yaohua Wang (National University of Defense Technology, China; Key Laboratory of Advanced Microprocessor Chips and Systems, China)</i>	

TATTOOED: A Robust Deep Neural Network Watermarking Scheme Based on Spread-Spectrum Channel Coding	1245
<i>Giulio Pagnotta (Sapienza University of Rome, Italy), Dorjan Hitaj (Sapienza University of Rome, Italy), Briland Hitaj (SRI International, USA), Fernando Perez-Cruz (Swiss Data Science Center, Switzerland), and Luigi V. Mancini (Sapienza University of Rome, Italy)</i>	
ViTGuard: Attention-Aware Detection against Adversarial Examples for Vision Transformer	1259
<i>Shihua Sun (Virginia Tech, USA), Kenechukwu Nwodo (Virginia Tech, USA), Shridatt Sugrim (Kryptowire Labs, USA), Angelos Stavrrou (Virginia Tech, USA; Kryptowire Labs, USA), and Haining Wang (Virginia Tech, USA)</i>	

Author Index