

2024 IEEE Symposium on Security and Privacy (SP 2024)

**San Francisco, California, USA
20-23 May 2024**

Pages 1-696



**IEEE Catalog Number: CFP24020-POD
ISBN: 979-8-3503-3131-8**

**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:	CFP24020-POD
ISBN (Print-On-Demand):	979-8-3503-3131-8
ISBN (Online):	979-8-3503-3130-1
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

CURRAN ASSOCIATES INC.
proceedings
.com

2024 IEEE Symposium on Security and Privacy (SP) SP 2024

Table of Contents

Message from the General Chair	xl
Message from the Program Chairs	xliii
Organizing Committee	xliv
External Reviewers	xlvii

Track 1 - Session 1: Scams and Phishing

On SMS Phishing Tactics and Infrastructure	1
<i>Aleksandr Nahapetyan (North Carolina State University), Sathvik Prasad (North Carolina State University), Kevin Childs (North Carolina State University), Adam Oest (Paypal, Inc.), Yeganeh Ladwig (Paypal, Inc.), Alexandros Kapravelos (North Carolina State University), and Brad Reeves (North Carolina State University)</i>	
Conning the Crypto Conman: End-to-End Analysis of Cryptocurrency-based Technical Support Scams	17
<i>Bhupendra Acharya (CISPA Helmholtz Center for Information Security), Muhammad Saad (PayPal Inc.), Antonio Emanuele Cinà (Università di Genova), Lea Schönherr (CISPA Helmholtz Center for Information Security), Hoang Dai Nguyen (Louisiana State University), Adam Oest (PayPal Inc.), Phani Vadrevu (Louisiana State University), and Thorsten Holz (CISPA Helmholtz Center for Information Security)</i>	
From Chatbots to Phishbots?: Phishing Scam Generation in Commercial Large Language Models ...	36
<i>Sayak Saha Roy (University of Texas at Arlington, USA), Poojitha Thota (University of Texas at Arlington, USA), Krishna Vamsi Naragam (University of Texas at Arlington, USA), and Shirin Nilizadeh (University of Texas at Arlington, USA)</i>	

Track 2 - Session 1: Deep Fakes

A Representative Study on Human Detection of Artificially Generated Media Across Countries.....	55
<i>Joel Frank (Ruhr-Universität Bochum), Franziska Herbert (Ruhr-Universität Bochum), Jonas Ricker (Ruhr-Universität Bochum), Lea Schönherr (CISPA Helmholtz Center for Information Security), Thorsten Eisenhofer (TU Berlin), Asja Fischer (Ruhr-Universität Bochum), Markus Dürmuth (Leibniz Universität Hannover), and Thorsten Holz (CISPA Helmholtz Center for Information Security)</i>	

AVA: Inconspicuous Attribute Variation-based Adversarial Attack bypassing DeepFake Detection	74
<i>Xiangtao Meng (Shandong University, China), Li Wang (Shandong University, China), Shanqing Guo (Shandong University, China), Lei Ju (Shandong University, China), and Qingchuan Zhao (City University of Hong Kong, China)</i>	

An Analysis of Recent Advances in Deepfake Image Detection in an Evolving Threat Landscape.....	91
<i>Sifat Muhammad Abdullah (Virginia Tech, USA), Aravind Cheruou (Virginia Tech, USA), Shrayya Kanchi (Virginia Tech, USA), Taejoong Chung (Virginia Tech, USA), Peng Gao (Virginia Tech, USA), Murtuza Jadliwala (UT San Antonio, USA), and Bimal Viswanath (Virginia Tech, USA)</i>	

Track 3 - Session 1: Privacy for Datasets

DP-Auditorium: A Large Scale Library for Auditing Differential Privacy	110
<i>William Kong (Google), Andres Muñoz Medina (Google), Monica Ribero (Google), and Umar Syed (Google)</i>	
Time-Aware Projections: Truly Node-Private Graph Statistics under Continual Observation	127
<i>Connor Wagaman (Boston University), Palak Jain (Boston University), and Adam Smith (Boston University)</i>	
Synq: Public Policy Analytics Over Encrypted Data	146
<i>Zachary Espiritu (MongoDB Research), Marilyn George (MongoDB Research), Seny Kamara (MongoDB Research and Brown University), and Lucy Qin (Brown University)</i>	

Track 1 - Session 2: Web Security

The Great Request Robbery: An Empirical Study of Client-side Request Hijacking Vulnerabilities on the Web	166
<i>Soheil Khodayari (CISPA Helmholtz Center for Information Security), Thomas Barber (SAP Security Research), and Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security)</i>	
Break the Wall from bottom: Automated Discovery of Protocol-Level Evasion Vulnerabilities in Web Application Firewalls	185
<i>Qi Wang (Tsinghua University, China), Jianjun Chen (Tsinghua University and Zhongguancun Laboratory, China), Zheyu Jiang (Tsinghua University, China), Run Guo (Tsinghua University, China), Ximeng Liu (Fuzhou University, China), Chao Zhang (Tsinghua University and Zhongguancun Laboratory, China), and Haixin Duan (Tsinghua University and Zhongguancun Laboratory, China)</i>	
Parse Me, Baby, One More Time: Bypassing HTML Sanitizer via Parsing Differentials	203
<i>David Klein (Technische Universität Braunschweig) and Martin Johns (Technische Universität Braunschweig)</i>	

Holistic Concolic Execution for Dynamic Web Applications via Symbolic Interpreter Analysis.....	222
<i>Penghui Li (Zhongguancun Laboratory, China), Wei Meng (The Chinese University of Hong Kong, China), Mingxue Zhang (Zhejiang University, China), Chenlin Wang (The Chinese University of Hong Kong, China), and Changhua Luo (The Chinese University of Hong Kong, China)</i>	
Where URLs Become Weapons: Automated Discovery of SSRF Vulnerabilities in Web Applications.....	239
<i>Enze Wang (National University of Defense Technology & Tsinghua University, China), Jianjun Chen (Tsinghua University & Zhongguancun Laboratory, China), Wei Xie (National University of Defense Technology, China), Chuhan Wang (Tsinghua University, China), Yifei Gao (National University of Defense Technology, China), Zhenhua Wang (National University of Defense Technology, China), Haixin Duan (Tsinghua University & Zhongguancun Laboratory, China), Yang Liu (Nanyang Technological University, Singapore), and Baosheng Wang (National University of Defense Technology)</i>	
SINBAD: Saliency-informed detection of breakage caused by ad blocking	258
<i>Saiid El Hajj Chehade (EPFL, Switzerland), Sandra Siby (Imperial College London, United Kingdom), and Carmela Troncoso (EPFL, Switzerland)</i>	
C-FRAME: Characterizing and measuring in-the-wild CAPTCHA attacks	277
<i>Hoang Dai Nguyen (Louisiana State University), Karthika Subramani (Georgia Institute of Technology), Bhupendra Acharya (CISPA Helmholtz Center for Information Security), Roberto Perdisci (University of Georgia), and Phani Vadrevu (Louisiana State University)</i>	
JASMINE: Scale up JavaScript Static Security Analysis with Computation-based Semantic Explanation	296
<i>Feng Xiao (Georgia Institute of Technology), Zhongfu Su (Wuhan University), Guangliang Yang (Fudan University), and Wenke Lee (Georgia Institute of Technology)</i>	

Track 2 - Session 2: Security in the Real World

A Tale of Two Indostroyers: It was the Season of Darkness	312
<i>Luis Salazar (University of California, Santa Cruz), Sebastian Castro (University of California, Santa Cruz), Juan Lozano (University of California, Santa Cruz), Keerthi Koneru (University of California, Santa Cruz), Emmanuele Zambon (Eindhoven University of Technology), Bing Huang (The University of Texas at Austin), Ross Baldick (The University of Texas at Austin), Marina Krotofil (Information Systems Security Partners), Alonso Rojas (Axon Group), and Alvaro Cardenas (University of California, Santa Cruz)</i>	
AquaSonic: Acoustic Manipulation of Underwater Data Center Operations and Resource Management	331
<i>Jennifer Sheldon (University of Florida), Weidong Zhu (University of Florida), Adnan Abdullah (University of Florida), Sri Hrushikesh Varma Bhupathiraju (University of Florida), Takeshi Sugawara (The University of Electro-Communications), Kevin Butler (University of Florida), Jahidul Islam (University of Florida), and Sara Rampazzi (University of Florida)</i>	

“Watching over the shoulder of a professional”: Why hackers make mistakes and how they fix them	350
<i>Irina Ford (Arizona State University), Ananta Soneji (asonjei@asu.edu), Faris Bugra Kokulu (Arizona State University), Jayakrishna Vadayath (Arizona State University), Zion Leonahenahe Basque (Arizona State University), Gaurav Vipat (Arizona State University), Adam Doupe (Arizona State University), Ruoyu Wang (Arizona State University), Gail-Joon Ahn (Arizona State University), Tiffany Bao (Arizona State University), and Yan Shoshitaishvili (Arizona State University)</i>	
A Picture is Worth 500 Labels: A Case Study of Demographic Disparities in Local Machine Learning Models for Instagram and TikTok	369
<i>Jackson West (University of Wisconsin -- Madison), Lea Thiemt (Technical University of Munich), Shima Ahmed (University of Wisconsin -- Madison), Maggie Bartig (University of Wisconsin -- Madison), Kassem Fawaz (University of Wisconsin -- Madison), and Suman Banerjee (University of Wisconsin -- Madison)</i>	
MAWSEO: Adversarial Wiki Search Poisoning for Illicit Online Promotion	388
<i>Zilong Lin (Indiana University Bloomington, USA), Zhengyi Li (Indiana University Bloomington, USA), Xiaojing Liao (Indiana University Bloomington, USA), XiaoFeng Wang (Indiana University Bloomington, USA), and Xiaozhong Liu (Worcester Polytechnic Institute, USA)</i>	
Poisoning Web-Scale Training Datasets is Practical	407
<i>Nicholas Carlini (Google DeepMind), Matthew Jagielski (Google DeepMind), Christopher A. Choquette-Choo (Google DeepMind), Daniel Paleka (ETH Zurich), Will Pearce (NVIDIA), Hyrum Anderson (Robust Intelligence), Andreas Terzis (Google DeepMind), Kurt Thomas (Google), and Florian Tramèr (ETH Zurich)</i>	
Don't Shoot the Messenger: Localization Prevention of Satellite Internet Users	426
<i>David Koisser (Technical University of Darmstadt, Germany), Richard Mitev (Technical University of Darmstadt, Germany), Marco Chilese (Technical University of Darmstadt, Germany), and Ahmad-Reza Sadeghi (Technical University of Darmstadt, Germany)</i>	
The Dark Side of Scale: Insecurity of Direct-to-Cell Satellite Mega-Constellations	445
<i>Wei Liu (Tsinghua University), Yuanjie Li (Tsinghua University), Hewu Li (Tsinghua University), Yimei Chen (Tsinghua University), Yufeng Wang (Tsinghua University), Jingyi Lan (Tsinghua University), Jianping Wu (Tsinghua University), Qian Wu (Tsinghua University), Jun Liu (Tsinghua University), and Zeqi Lai (Tsinghua University)</i>	

Track 3 - Session 2: Crypto with Others

SoK: Collusion-resistant Multi-party Private Set Intersections in the Semi-honest Model	465
<i>Jelle Vos (Delft University of Technology), Mauro Conti (University of Padua), and Zekeriya Erkin (Delft University of Technology)</i>	

GAuV: A Graph-Based Automated Verification Framework for Perfect Semi-Honest Security of Multiparty Computation Protocols	484
<i>Xingyu Xie (Tsinghua University; RealAI), Yifei Li (Tsinghua University), Wei Zhang (Tsinghua University), Tuowei Wang (Tsinghua University), Shizhen Xu (RealAI), Jun Zhu (Tsinghua University; RealAI), and Yifan Song (Tsinghua University)</i>	
Don't Eject the Impostor: Fast Three-Party Computation With a Known Cheater	503
<i>Andreas Brüggemann (Technical University of Darmstadt, Germany), Oliver Schick (Technical University of Darmstadt, Germany), Thomas Schneider (Technical University of Darmstadt, Germany), Ajith Suresh (Technology Innovation Institute, Abu Dhabi), and Hossein Yalame (Technical University of Darmstadt, Germany)</i>	
Scalable Mixed-Mode MPC	523
<i>Radhika Garg (Northwestern University), Kang Yang (State Key Laboratory of Cryptology), Jonathan Katz (University of Maryland), and Xiao Wang (Northwestern University)</i>	
Asterisk: Super-fast MPC with a Friend	542
<i>Banashri Karmakar (Indian Institute of Science, India), Nishat Koti (Indian Institute of Science, India), Arpita Patra (Indian Institute of Science, India), Sikhar Patranabis (IBM Research, India), Protik Paul (Indian Institute of Science, India), and Divya Ravi (Aarhus University, Denmark)</i>	
Efficient Actively Secure DPF and RAM-based 2PC with One-Bit Leakage	561
<i>Wenhao Zhang (Northwestern University, USA), Xiaojie Guo (Nankai University and State Key Laboratory of Cryptology, China), Kang Yang (State Key Laboratory of Cryptology, China), Ruiyu Zhu (No Affiliation), Yu Yu (Shanghai Jiao Tong University and Shanghai Qi Zhi Institute, China), and Xiao Wang (Northwestern University, USA)</i>	
MPC-in-the-Head Framework without Repetition and its Applications to the Lattice-based Cryptography	578
<i>WeiHao Bai (Institute of Software Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Long Chen (Institute of Software Chinese Academy of Sciences, China), Qianwen Gao (Institute of Software Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), and Zhenfeng Zhang (Institute of Software Chinese Academy of Sciences, China)</i>	
Orca: FSS-based Secure Training and Inference with GPUs	597
<i>Neha Jawalkar (Indian Institute of Science, India), Kanav Gupta (Microsoft Research, India), Arkaprava Basu (Indian Institute of Science, India), Nishanth Chandran (Microsoft Research, India), Divya Gupta (Microsoft Research, India), and Rahul Sharma (Microsoft Research, India)</i>	

Track 1 - Session 3: Humans

Security, Privacy, and Data-sharing Trade-offs When Moving to the United States: Insights from a Qualitative Study	617
<i>Mindy Tran (Paderborn University, The George Washington University), Collins W. Munyendo (The George Washington University), Harshini Sri Ramulu (Paderborn University, The George Washington University), Rachel Gonzalez Rodriguez (The George Washington University), Luisa Ball Schnell (The George Washington University), Cora Sula (The George Washington University), Lucy Simko (The George Washington University), and Yasemin Acar (Paderborn University, The George Washington University)</i>	
SoK: Safer Digital-Safety Research Involving At-Risk Users	635
<i>Rosanna Bellini (Cornell Tech, USA), Emily Tseng (Cornell Tech, USA), Noel Warford (University of Maryland, USA), Alaa Daffalla (Cornell Tech, USA), Tara Matthews (Google, USA), Sunny Consolvo (Google, USA), Jill Palzkill Woelfer (JumpCloud, USA), Patrick Gage Kelley (Google, USA), Michelle L. Mazurek (University of Maryland, USA), Dana Cuomo (Lafayette College, USA), Nicola Dell (Cornell Tech, USA), and Thomas Ristenpart (Cornell Tech, USA)</i>	
Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution	655
<i>Kasra EdalatNejad (EPFL, Switzerland), Wouter Lueks (CISPA Helmholtz Center for Information Security, Germany), Justinas Sukaitis (International Committee of the Red Cross, Switzerland), Vincent Graf Narbel (International Committee of the Red Cross, Switzerland), Massimo Marelli (International Committee of the Red Cross, Switzerland), and Carmela Troncoso (EPFL, Switzerland)</i>	
SoK: Technical Implementation and Human Impact of Internet Privacy Regulations	673
<i>Eleanor Birrell (Pomona College), Jay Rodolitz (Northeastern University), Angel Ding (Wellesley College), Jenna Lee (University of Washington), Emily McReynolds (Future of Privacy Forum), Jevan Hutson (Hintze Law PLLC), and Ada Lerner (Northeastern University)</i>	
Digital Security — A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups	697
<i>Franziska Herbert (Ruhr University Bochum, Germany), Steffen Becker (Ruhr University Bochum, Germany; Max Planck Institute for Security and Privacy, Germany), Annalina Buckmann (Ruhr University Bochum, Germany), Marvin Kowalewski (Ruhr University Bochum, Germany), Jonas Hielscher (Ruhr University Bochum, Germany), Yasemin Acar (Paderborn University, Germany), Markus Dürmuth (Hannover University, Germany), Yixin Zou (Max Planck Institute for Security and Privacy, Germany), and M. Angela Sasse (Ruhr University Bochum, Germany)</i>	
No Easy Way Out: the Effectiveness of Deplatforming an Extremist Forum to Suppress Hate and Harassment	717
<i>Anh V. Vu (University of Cambridge), Alice Hutchings (University of Cambridge), and Ross Anderson (University of Cambridge and University of Edinburgh)</i>	

Withdrawing is believing? Detecting Inconsistencies Between Withdrawal Choices and Third-party Data Collections in Mobile Apps	735
<i>Xiaolin Du (Fudan University), Zhemin Yang (Fudan University), Jiapeng Lin (Fudan University), Yinzhi Cao (Johns Hopkins University), and Min Yang (Fudan University)</i>	
The Role of User-Agent Interactions on Mobile Money Practices in Kenya and Tanzania	752
<i>Karen Sowon (Carnegie Mellon University), Edith Luhanga (Carnegie Mellon University-Africa), Lorrie Faith Cranor (Carnegie Mellon University), Giulia Fanti (Carnegie Mellon University), Conrad Tucker (Carnegie Mellon University), and Assane Gueye (Carnegie Mellon University-Africa)</i>	

Track 2 - Session 3: LLMs and Security

You Only Prompt Once: On the Capabilities of Prompt Learning on Large Language Models to Tackle Toxic Content	770
<i>Xinlei He (CISPA Helmholtz Center for Information Security, Germany), Savvas Zannettou (TU Delft, Netherlands), Yun Shen (NetApp, UK), and Yang Zhang (CISPA Helmholtz Center for Information Security, Germany)</i>	
Moderating New Waves of Online Hate with Chain-of-Thought Reasoning in Large Language Models	788
<i>Nishant Vishwamitra (University of Texas at San Antonio, USA), Keyan Guo (University at Buffalo, USA), Farhan Tajwar Romit (University of Texas at San Antonio, USA), Isabelle Ondracek (University at Buffalo, USA), Long Cheng (Clemson University, USA), Ziming Zhao (University at Buffalo, USA), and Hongxin Hu (University at Buffalo, USA)</i>	
Nightshade: Prompt-Specific Poisoning Attacks on Text-to-Image Generative Models	807
<i>Shawn Shan (University of Chicago), Wenxin Ding (University of Chicago), Josephine Passananti (University of Chicago), Stanley Wu (University of Chicago), Haitao Zheng (University of Chicago), and Ben Y. Zhao (University of Chicago)</i>	
On Large Language Models' Resilience to Coercive Interrogation	826
<i>Zhuo Zhang (Purdue University, USA), Guangyu Shen (Purdue University, USA), Guanhong Tao (Purdue University, USA), Siyuan Cheng (Purdue University, USA), and Xiangyu Zhang (Purdue University, USA)</i>	
PromptCARE: Prompt Copyright Protection by Watermark Injection and Verification	845
<i>Hongwei Yao (Zhejiang University), Jian Lou (ZJU-Hangzhou Global Scientific and Technological Innovation Center), Zhan Qin (Zhejiang University), and Kui Ren (Zhejiang University)</i>	
LLMs Cannot Reliably Identify and Reason About Security Vulnerabilities (Yet?): A Comprehensive Evaluation, Framework, and Benchmarks	862
<i>Saad Ullah (Boston University), Mingji Han (Boston University), Saurabh Pujar (IBM Research), Hammond Pearce (UNSW Sydney), Ayse Coskun (Boston University), and Gianluca Stringhini (Boston University)</i>	

LLMIF: Augmented Large Language Model for Fuzzing IoT Devices	881
<i>Jincheng Wang (The Hong Kong Polytechnic University, China), Le Yu (Nanjing University of Posts and Telecommunications, China), and Xiapu Luo (The Hong Kong Polytechnic University, China)</i>	
SneakyPrompt: Jailbreaking Text-to-image Generative Models	897
<i>Yuchen Yang (Johns Hopkins University), Bo Hui (Johns Hopkins University), Haolin Yuan (Johns Hopkins University), Neil Gong (Duke University), and Yinzhi Cao (Johns Hopkins University)</i>	

Track 3 - Session 3: Differential Privacy

Eureka: A General Framework for Black-box Differential Privacy Estimators	913
<i>Yun Lu (University of Victoria), Malik Magdon-Ismail (Rensselaer Polytechnic Institute), Yu Wei (Purdue University), and Vassilis Zikas (Purdue University)</i>	
Casual Users and Rational Choices within Differential Privacy	932
<i>Narges Ashena (University of Zurich), Oana Inel (University of Zurich), Badrie L. Persaud (University of Zurich), and Abraham Bernstein (University of Zurich)</i>	
Lower Bounds for Rényi Differential Privacy in a Black-Box Setting	951
<i>Tim Kutta (Ruhr-University Bochum), Önder Askin (Ruhr-University Bochum), and Martin Dunsche (Ruhr-University Bochum)</i>	
Bounded and Unbiased Composite Differential Privacy	972
<i>Kai Zhang (Swinburne University of Technology), Yanjun Zhang (University of Technology Sydney and CSIRO's Data61), Ruoxi Sun (CSIRO's Data61), Pei-Wei Tsai (Swinburne University of Technology), Muneeb Ul Hassan (Deakin University), Xin Yuan (CSIRO's Data61), Minhui Xue (CSIRO's Data61), and Jinjun Chen (Swinburne University of Technology)</i>	
Cohere: Managing Differential Privacy in Large Scale Systems	991
<i>Nicolas Küchler (ETH Zurich, Switzerland), Emanuel Opel (ETH Zurich, Switzerland), Hidde Lycklama (ETH Zurich, Switzerland), Alexander Viand (Intel Labs, Switzerland), and Anwar Hithnawi (ETH Zurich, Switzerland)</i>	
DPI: Ensuring Strict Differential Privacy for Infinite Data Streaming	1009
<i>Shuya Feng (University of Connecticut, USA), Meisam Mohammady (Iowa State University, USA), Han Wang (University of Kansas, USA), Xiaochen Li (Zhejiang University, China), Zhan Qin (Zhejiang University, China), and Yuan Hong (University of Connecticut, USA)</i>	
Budget Recycling Differential Privacy	1028
<i>Bo Jiang (TikTok Inc.), Jian Du (TikTok Inc.), Sagar Sharma (TikTok Inc), and Qiang Yan (TikTok Inc.)</i>	

Measure-Observe-Remeasure: An Interactive Paradigm for Differentially-Private Exploratory Analysis	1047
<i>Priyanka Nanayakkara (Northwestern University, USA), Hyeok Kim (Northwestern University, USA), Yifan Wu (Northwestern University, USA), Ali Saroghah (University of Massachusetts Amherst, USA), Narges Mahyar (University of Massachusetts Amherst, USA), Gerome Miklau (University of Massachusetts Amherst, USA), and Jessica Hullman (Northwestern University, USA)</i>	

Track 1 - Session 4: Software Supply Chain

Everyone for Themselves? A Qualitative Study about Individual Security Setups of Open Source Software Contributors	1065
<i>Sabrina Amft (CISPA Helmholtz Center for Information Security, Germany), Sandra Höltervenhoff (Leibniz University Hannover, Germany), Rebecca Panskus (Ruhr University Bochum, Germany), Karola Marky (Ruhr University Bochum, Germany), and Sascha Fahl (CISPA Helmholtz Center for Information Security, Germany)</i>	
Measuring the Effects of Stack Overflow Code Snippet Evolution on Open-Source Software Security	1083
<i>Alfusaimey Jallow (CISPA Helmholtz Center for Information Security, Germany), Michael Schilling (CISPA Helmholtz Center for Information Security, Germany), Michael Backes (CISPA Helmholtz Center for Information Security, Germany), and Soen Bugiel (CISPA Helmholtz Center for Information Security, Germany)</i>	
Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities	1102
<i>Julia Wunder (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), Andreas Kurtz (Heilbronn University of Applied Sciences, Germany), Christian Eichenmüller (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), Freya Gassmann (Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau, Germany), and Zinaida Benenson (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)</i>	
TROJANPUZZLE: Covertly Poisoning Code-Suggestion Models	1122
<i>Hojjat Aghakhani (University of California, Santa Barbara), Wei Dai (Microsoft Corporation), Andre Manoel (Microsoft Corporation), Xavier Fernandes (Microsoft Corporation), Anant Kharkar (Microsoft Corporation), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California, Santa Barbara), David Evans (University of Virginia), Ben Zorn (Microsoft Corporation), and Robert Sim (Microsoft Corporation)</i>	
Poisoned ChatGPT Finds Work for Idle Hands: Exploring Developers' Coding Practices with Insecure Suggestions from Poisoned AI Models	1141
<i>Sanghak Oh (Sungkyunkwan University, Republic of Korea), Kiho Lee (Sungkyunkwan University, Republic of Korea), Seonhye Park (Sungkyunkwan University, Republic of Korea), Doowon Kim (University of Tennessee, USA), and Hyoungshick Kim (Sungkyunkwan University, Republic of Korea)</i>	

Signing in Four Public Software Package Registries: Quantity, Quality, and Influencing Factors	1160
<i>Taylor R. Schorlemmer (Purdue University), Kelechi G. Kalu (Purdue University), Luke Chigges (Purdue University), Kyung Myung Ko (Purdue University), Eman Abu Ishgair (Purdue University), Saurabh Bagchi (Purdue University), Santiago Torres-Arias (Purdue University), and James C. Davis (Purdue University)</i>	
More Haste, Less Speed: Cache Related Security Threats in Continuous Integration Services	1179
<i>Yacong Gu (Tsinghua University; Tsinghua University-QI-ANXIN Group JCNS, China), Lingyun Ying (QI-ANXIN Technology Research Institute; Tsinghua University-QI-ANXIN Group JCNS, China), Huajun Chai (QI-ANXIN Technology Research Institute, China), Yingyuan Pu (QI-ANXIN Technology Research Institute, China), Haixin Duan (BNRist & Institute for Network Science and Cyberspace, Tsinghua University; Tsinghua University-QI-ANXIN Group JCNS, China), and Xing Gao (University of Delaware, USA)</i>	
Patchy Performance? Uncovering the Vulnerability Management Practices of IoT-Centric Vendors	1198
<i>Sandra Rivera Pérez (Delft University of Technology), Michel van Eeten (Delft University of Technology), and Carlos H. Gañán (Delft University of Technology)</i>	

Track 2 - Session 4: ML Attacks

Need for Speed: Taming Backdoor Attacks with Speed and Precision	1217
<i>Zhuo Ma (Xidian University), Yilong Yang (Xidian University), Yang Liu (Xidian University), Tong Yang (Peking University), Xinjing Liu (Xidian University), Teng Li (Xidian University), and Zhan Qin (Zhejiang University)</i>	
Multi-instance Adversarial Attack on GNN-Based Malicious Domain Detection	1236
<i>Mahmoud Nazzal (New Jersey Institute of Technology, USA), Issa Khalil (Qatar Computing Research Institute (QCRI), Hamad Bin Khalifa University (HBKU), Qatar), Abdallah Khreishah (New Jersey Institute of Technology, USA), NhatHai Phan (New Jersey Institute of Technology, USA), and Yao Ma (New Jersey Institute of Technology, USA)</i>	
Dropout Attacks	1255
<i>Andrew Yuan (Northeastern University, USA), Alina Oprea (Northeastern University, USA), and Cheng Tan (Northeastern University, USA)</i>	
BounceAttack: A Query-Efficient Decision-based Adversarial Attack by Bouncing into the Wild	1270
<i>Jie Wan (Zhejiang University), Jianhao Fu (Zhejiang University), Lijin Wang (Zhejiang University), and Ziqi Yang (Zhejiang University; ZJU-Hangzhou Global Scientific and Technological Innovation Center)</i>	

LOKI: Large-scale Data Reconstruction Attack against Federated Learning through Model Manipulation	1287
<i>Joshua Christian Zhao (Purdue University), Atul Sharma (Purdue University), Ahmed Roushdy Elkordy (University of Southern California), Yahya H. Ezzeldin (University of Southern California), Salman Avestimehr (University of Southern California), and Saurabh Bagchi (Purdue University)</i>	
Test-Time Poisoning Attacks Against Test-Time Adaptation Models	1306
<i>Tianshuo Cong (Tsinghua University), Xinlei He (CISPA Helmholtz Center for Information Security), Yun Shen (NetApp), and Yang Zhang (CISPA Helmholtz Center for Information Security)</i>	
Attacking Byzantine Robust Aggregation in High Dimensions	1325
<i>Sarthak Choudhary (National University of Singapore), Aashish Kolluri (National University of Singapore), and Prateek Saxena (National University of Singapore)</i>	
CaFA: Cost-aware, Feasible Attacks With Database Constraints Against Neural Tabular Classifiers	1345
<i>Matan Ben-Tov (Tel Aviv University), Daniel Deutch (Tel Aviv University), Nave Frost (eBay), and Mahmood Sharif (Tel Aviv University)</i>	

Track 3 - Session 4: Passwords and Authentication

Universal Neural-Cracking-Machines: Self-Configurable Password Models from Auxiliary Data ..	1365
<i>Dario Pasquini (SPRING Lab; EPFL, Switzerland), Giuseppe Ateniese (George Mason University), and Carmela Troncoso (SPRING Lab; EPFL, Switzerland)</i>	
PassREfinder: Credential Stuffing Risk Prediction by Representing Password Reuse between Websites on a Graph	1385
<i>Jaehan Kim (Korea Advanced Institute of Science and Technology (KAIST), Korea), Minkyoo Song (Korea Advanced Institute of Science and Technology (KAIST), Korea), Minjae Seo (Korea Advanced Institute of Science and Technology (KAIST), Korea), Youngjin Jin (Korea Advanced Institute of Science and Technology (KAIST), Korea), and Seungwon Shin (Korea Advanced Institute of Science and Technology (KAIST), Korea)</i>	
Breach Extraction Attacks: Exposing and Addressing the Leakage in Second Generation Compromised Credential Checking Services	1405
<i>Dario Pasquini (EPFL, Switzerland), Danilo Francati (Aarhus University, Denmark), Giuseppe Ateniese (George Mason University, Virginia), and Evgenios M. Kornaropoulos (George Mason University, Virginia)</i>	
A Security Analysis of Honey Vaults	1424
<i>Fei Duan (Nankai University, China), Ding Wang (Nankai University), and Chunfu Jia (Nankai University, China)</i>	

Combing for Credentials: Active Pattern Extraction from Smart Reply	1443
<i>Bargav Jayaraman (University of Virginia), Esha Ghosh (Microsoft Research), Melissa Chase (Microsoft Research), Sambuddha Roy (Microsoft), Wei Dai (Microsoft Research), and David Evans (University of Virginia)</i>	
ARMOR: A Formally Verified Implementation of X.509 Certificate Chain Validation	1462
<i>Joyanta Debnath (Stony Brook University), Christa Jenkins (Stony Brook University), Yuteng Sun (The Chinese University of Hong Kong), Sze Yiu Chau (The Chinese University of Hong Kong), and Omar Chowdhury (Stony Brook University)</i>	
DY Fuzzing: Formal Dolev-Yao Models Meet Cryptographic Protocol Fuzz Testing	1481
<i>Max Ammann (Independent Researcher & Trail of Bits, Germany), Lucca Hirschi (Inria Nancy Grand-Est, Université de Lorraine, LORIA, France), and Steve Kremer (Inria Nancy Grand-Est, Université de Lorraine, LORIA, France)</i>	
To Auth or Not To Auth? A Comparative Analysis of the Pre- and Post-Login Security Landscape	1500
<i>Jannis Rautenstrauch (CISPA Helmholtz Center for Information Security, Germany), Metodi Mitkov (CISPA Helmholtz Center for Information Security, Germany), Thomas Helbrecht (CISPA Helmholtz Center for Information Security, Germany), Lorenz Hetterich (CISPA Helmholtz Center for Information Security, Germany), and Ben Stock (CISPA Helmholtz Center for Information Security, Germany)</i>	

Track 1 - Session 5: Being Secure Online

Targeted and Troublesome: Tracking and Advertising on Children’s Websites	1517
<i>Zahra Moti (Radboud University, The Netherlands), Asuman Senol (KU Leuven, Belgium), Hamid Bostani (Radboud University, The Netherlands), Frederik Zuiderveen Borgesius (Radboud University, The Netherlands), Veelasha Moonsamy (Ruhr University Bochum, Germany), Arunesh Mathur (Independent Researcher), and Gunes Acar (Radboud University, The Netherlands)</i>	
Children, Parents, and Misinformation on Social Media	1536
<i>Filipo Sharevski (DePaul University) and Jennifer Vander Loop (DePaul University)</i>	
Understanding Parents’ Perceptions and Practices Toward Children’s Security and Privacy in Virtual Reality	1554
<i>Jiaxun Cao (Duke Kunshan University), Abhinaya S.B. (North Carolina State University), Anupam Das (North Carolina State University), and Pardis Emami-Naeini (Duke University)</i>	
The Times They Are A-Changin’: Characterizing Post-Publication Changes to Online News	1573
<i>Chris Tsoukaladelis (Stony Brook University, USA), Brian Kondracki (Stony Brook University, USA), Niranjana Balasubramanian (Stony Brook University, USA), and Nick Nikiforakis (Stony Brook University, USA)</i>	

The Inventory is Dark and Full of Misinformation: Understanding Ad Inventory Pooling in the Ad-Tech Supply Chain	1590
<i>Yash Vekaria (University of California, Davis), Rishab Nithyanand (University of Iowa), and Zubair Shafiq (University of California, Davis)</i>	
Specious Sites: Tracking the Spread and Sway of Spurious News Stories at Scale	1609
<i>Hans Hanley (Stanford University), Deepak Kumar (Stanford University), and Zakir Durumeric (Stanford University)</i>	

Track 2 - Session 5: ML Security for Audio and Video

ALIF: Low-Cost Adversarial Audio Attacks on Black-Box Speech Platforms using Linguistic Features	1628
<i>Peng Cheng (Zhejiang University, China; ZJU-Hangzhou Global Scientific and Technological Innovation Center, China), Yuwei Wang (Zhejiang University, China; ZJU-Hangzhou Global Scientific and Technological Innovation Center, China), Peng Huang (Zhejiang University, China; ZJU-Hangzhou Global Scientific and Technological Innovation Center, China), Zhongjie Ba (Zhejiang University, China; ZJU-Hangzhou Global Scientific and Technological Innovation Center, China), Xiaodong Lin (University of Guelph, Canada), Feng Lin (Zhejiang University, China; ZJU-Hangzhou Global Scientific and Technological Innovation Center, China), Li Lu (Zhejiang University, China; ZJU-Hangzhou Global Scientific and Technological Innovation Center, China), and Kui Ren (Zhejiang University, China; ZJU-Hangzhou Global Scientific and Technological Innovation Center, China)</i>	
FlowMur: A Stealthy and Practical Audio Backdoor Attack with Limited Knowledge	1646
<i>Jiahe Lan (Xidian University, China), Jie Wang (Xidian University, China), Baochen Yan (Xidian University, China), Zheng Yan (Xidian University, China), and Elisa Bertino (Purdue University, USA)</i>	
Understanding and Benchmarking the Commonality of Adversarial Examples	1665
<i>Ruiwen He (Zhejiang University, China), Yushi Cheng (Zhejiang University, China), Junning Ze (Zhejiang University, China), Xiaoyu Ji (Zhejiang University, China), and Wenyuan Xu (Zhejiang University, China)</i>	
Scores Tell Everything about Bob: Non-adaptive Face Reconstruction on Face Recognition Systems	1684
<i>Sunpill Kim (Hanyang University, Republic of Korea and Institute for Infocomm Research (I2R), A*STAR, Singapore), Yong Kiam Tan (Institute for Infocomm Research (I2R), A*STAR, Singapore), Bora Jeong (Hanyang University, Republic of Korea and Institute for Infocomm Research (I2R), A*STAR, Singapore), Soumik Mondal (Institute for Infocomm Research (I2R), A*STAR, Singapore), Mi Mi Aung Khin (Institute for Infocomm Research (I2R), A*STAR, Singapore), and Jae Hong Seo (Hanyang University, Republic of Korea)</i>	

ODSCAN: Backdoor Scanning for Object Detection Models	1703
<i>Siyuan Cheng (Purdue University, USA), Guangyu Shen (Purdue University, USA), Guanhong Tao (Purdue University, USA), Kaiyuan Zhang (Purdue University, USA), Zhuo Zhang (Purdue University, USA), Shengwei An (Purdue University, USA), Xiangzhe Xu (Purdue University, USA), Yingqi Liu (Microsoft, USA), Shiqing Ma (University of Massachusetts, Amherst, USA), and Xiangyu Zhang (Purdue University, USA)</i>	
Transferable Multimodal Attack on Vision-Language Pre-training Models	1722
<i>Haodi Wang (Southeast University), Kai Dong (Southeast University), Zhilei Zhu (Data Space Research Institute of Hefei Comprehensive National Science Centre), Haotong Qin (Beihang University), Aishan Liu (Beihang University), Xiaolin Fang (Southeast University), Jiakai Wang (Zhongguancun Laboratory), and Xianglong Liu (Beihang University)</i>	

Track 3 - Session 5: Zero Knowledge

Certifying Zero-Knowledge Circuits with Refinement Types	1741
<i>Junrui Liu (University of California, Santa Barbara, USA), Ian Kretz (The University of Texas at Austin, USA), Hanzhi Liu (University of California, Santa Barbara, USA; Veridise Inc., USA), Bryan Tan (Veridise Inc., USA), Jonathan Wang (Axiom, USA), Yi Sun (Axiom, USA), Luke Pearson (Polychain Capital, USA), Anders Miltner (Simon Fraser University, Canada), Isil Dillig (The University of Texas at Austin, USA; Veridise Inc., USA), and Yu Feng (University of California, Santa Barbara, USA; Veridise Inc., USA)</i>	
Ligetrn: Lightweight Scalable End-to-End Zero-Knowledge Proofs. Post-Quantum ZK-SNARKs on a Browser	1760
<i>Ruihan Wang (Ligero Inc), Carmit Hazay (Ligero Inc.), and Muthuramakrishnan Venkatasubramaniam (Ligero Inc.)</i>	
Pianist: Scalable zkRollups via Fully Distributed Zero-Knowledge Proofs	1777
<i>Tianyi Liu (University of Illinois Urbana-Champaign), Tiancheng Xie (UC Berkeley), Jiaheng Zhang (UC Berkeley), Dawn Song (UC Berkeley), and Yupeng Zhang (University of Illinois Urbana-Champaign)</i>	
Scalable Verification of Zero-Knowledge Protocols	1794
<i>Miguel Isabel (Complutense University of Madrid, Spain), Clara Rodríguez-Núñez (Complutense University of Madrid, Spain), and Albert Rubio (Complutense University of Madrid, Spain)</i>	
Efficient Zero-Knowledge Arguments For Paillier Cryptosystem	1813
<i>Borui Gong (The Hong Kong Polytechnic University, Hong Kong), Wang Fat Lau (The Hong Kong Polytechnic University, Hong Kong), Man Ho Au (The Hong Kong Polytechnic University, Hong Kong), Rupeng Yang (University of Wollongong, Australia), Haiyang Xue (The Hong Kong Polytechnic University, Hong Kong), and Lichun Li (Ant Group, China)</i>	
SwiftRange: A Short and Efficient Zero-Knowledge Range Argument For Confidential Transactions and More	1832
<i>Nan Wang (Australian National University and CSIRO's Data61, Australia), Sid Chi-Kin Chau (Australian National University and CSIRO's Data61, Australia), and Dongxi Liu (CSIRO's Data61, Australia)</i>	

Track 1 - Session 6: Fuzzing

Titan: Efficient Multi-target Directed Greybox Fuzzing	1849
<i>Heqing Huang (The Hong Kong University of Science and Technology), Peisen Yao (Zhejiang University), Hung-Chun Chiu (The Hong Kong University of Science and Technology), Yiyuan Guo (The Hong Kong University of Science and Technology), and Charles Zhang (The Hong Kong University of Science and Technology)</i>	
BENZENE: A Practical Root Cause Analysis System with an Under-Constrained State Mutation ..	1865
<i>Younggi Park (Korea University, Korea), Hwiwon Lee (Korea University, Korea), Jinho Jung (Ministry of National Defense, Korea), Hyungjoon Koo (Sungkyunkwan University, Korea), and Huy Kang Kim (Korea University, Korea)</i>	
Predecessor-aware Directed Greybox Fuzzing	1884
<i>Yujian Zhang (Southeast University), Yaokun Liu (Southeast University), Jinyu Xu (Southeast University), and Yanhao Wang (NIO)</i>	
AFGen: Whole-Function Fuzzing for Applications and Libraries	1901
<i>Yuwei Liu (University of Chinese Academy of Sciences, China), Yanhao Wang (Institute of Software Chinese Academy of Sciences, China), Xiangkun Jia (Institute of Software Chinese Academy of Sciences, China), Zheng Zhang (Ocean University of China, China), and Purui Su (Institute of Software Chinese Academy of Sciences, China)</i>	
LABRADOR: Response Guided Directed Fuzzing for Black-box IoT Devices	1920
<i>Hangtian Liu (Information Engineering University, China; Tsinghua University, China; Laboratory for Advanced Computing and Intelligence Engineering, China.), Shuitao Gan (Tsinghua University, China; Laboratory for Advanced Computing and Intelligence Engineering, China.), Chao Zhang (Tsinghua University, China; Zhongguancun Laboratory, China.), Zicong Gao (Information Engineering University, China; Tsinghua University, China; Laboratory for Advanced Computing and Intelligence Engineering, China.), Hongqi Zhang (Information Engineering University, China; Henan Key Laboratory of Information Security, China.), Xiangzhi Wang (University of Electronic Science and Technology of China, China), and Guangming Gao (Laboratory for Advanced Computing and Intelligence Engineering, China)</i>	
Chronos: Finding Timeout Bugs in Practical Distributed Systems by Deep-Priority Fuzzing with Transient Delay	1939
<i>Yuanliang Chen (Tsinghua University)</i>	
Everything is Good for Something: Counterexample-Guided Directed Fuzzing via Likely Invariant Inference	1956
<i>Heqing Huang (City University of Hong Kong, China), Anshunkang Zhou (The Hong Kong University of Science and Technology, China), Mathias Payer (École Polytechnique Fédérale de Lausanne, Switzerland), and Charles Zhang (The Hong Kong University of Science and Technology, China)</i>	

SoK: Prudent Evaluation Practices for Fuzzing	1974
<i>Moritz Schloegel (CISPA Helmholtz Center for Information Security), Nils Bars (CISPA Helmholtz Center for Information Security), Nico Schiller (CISPA Helmholtz Center for Information Security), Lukas Bernhard (CISPA Helmholtz Center for Information Security), Tobias Scharnowski (CISPA Helmholtz Center for Information Security), Addison Crump (CISPA Helmholtz Center for Information Security), Arash Ale-Ebrahim (CISPA Helmholtz Center for Information Security), Nicolai Bissantz (Ruhr University Bochum), Marius Muench (University of Birmingham), and Thorsten Holz (CISPA Helmholtz Center for Information Security)</i>	

Track 2 - Session 6: ML Backdoors

MM-BD: Post-Training Detection of Backdoor Attacks with Arbitrary Backdoor Pattern Types Using a Maximum Margin Statistic	1994
<i>Hang Wang (Anomalee Inc, USA; Pennsylvania State University, USA), Zhen Xiang (Anomalee Inc, USA; Pennsylvania State University, USA), David J. Miller (Anomalee Inc, USA; Pennsylvania State University, USA), and George Kesidis (Anomalee Inc, USA; Pennsylvania State University, USA)</i>	
BadVFL: Backdoor Attacks in Vertical Federated Learning	2013
<i>Mohammad Naseri (University College London), Yufei Han (INRIA Rennes), and Emiliano De Cristofaro (University of California, Riverside)</i>	
Distribution Preserving Backdoor Attack in Self-supervised Learning	2029
<i>Guanhong Tao (Purdue University, USA), Zhenting Wang (Rutgers University, USA), Shiwei Feng (Purdue University, USA), Guangyu Shen (Purdue University, USA), Shiqing Ma (University of Massachusetts Amherst, USA), and Xiangyu Zhang (Purdue University, USA)</i>	
Robust Backdoor Detection for Deep Learning via Topological Evolution Dynamics	2048
<i>Xiaoxing Mo (Deakin University), Yechao Zhang (Huazhong University of Science and Technology), Leo Yu Zhang (Griffith University), Wei Luo (Deakin University), Nan Sun (University of New South Wales Canberra), Shengshan Hu (Huazhong University of Science and Technology), Shang Gao (Deakin University), and Yang Xiang (Swinburne University of Technology)</i>	
DeepVenom: Persistent DNN Backdoors Exploiting Transient Weight Perturbations in Memories	2067
<i>Kunbei Cai (University of Central Florida, USA), Md Hafizul Islam Chowdhuryy (University of Central Florida, USA), Zhenkai Zhang (Clemson University, USA), and Fan Yao (University of Central Florida, USA)</i>	

BAFFLE: Hiding Backdoors in Offline Reinforcement Learning Datasets	2086
<i>Chen Gong (University of Virginia), Zhou Yang (Singapore Management University), Yunpeng Bai (Institute of Automation, Chinese Academy of Sciences), Jieke Shi (Singapore Management University), Junda He (Singapore Management University), Kecen Li (Institute of Automation, Chinese Academy of Sciences), Arunesh Sinha (Rutgers University), Bowen Xu (North Carolina State University), Xinwen Hou (Institute of Automation, Chinese Academy of Sciences), David Lo (Singapore Management University), and Tianhao Wang (University of Virginia)</i>	
Exploring the Orthogonality and Linearity of Backdoor Attacks	2105
<i>Kaiyuan Zhang (Purdue University, USA), Siyuan Cheng (Purdue University, USA), Guangyu Shen (Purdue University, USA), Guanhong Tao (Purdue University, USA), Shengwei An (Purdue University, USA), Anuran Makur (Purdue University, USA), Shiqing Ma (University of Massachusetts, Amherst, USA), and Xiangyu Zhang (Purdue University, USA)</i>	
BELT: Old-School Backdoor Attacks can Evade the State-of-the-Art Defense with Backdoor Exclusivity Lifting	2124
<i>Huming Qiu (Fudan University, China), Junjie Sun (Fudan University, China), Mi Zhang (Fudan University, China), Xudong Pan (Fudan University, China), and Min Yang (Fudan University, China)</i>	

Track 3 - Session 6: Blockchain I

Formal Model-Driven Analysis of Resilience of GossipSub to Attacks from Misbehaving Peers	2142
<i>Ankit Kumar (Northeastern University), Max von Hippel (Northeastern University), Panagiotis Manolios (Northeastern University), and Cristina Nita-Rotaru (Northeastern University)</i>	
Larger-scale Nakamoto-style Blockchains Don't Necessarily Offer Better Security	2161
<i>Jannik Albrecht (Ruhr University Bochum), Sebastien Andreina (NEC Laboratories Europe), Frederik Armknecht (University of Mannheim), Ghassan Karame (Ruhr University Bochum), Giorgia Marson (NEC Laboratories Europe), and Julian Willingmann (Ruhr University Bochum)</i>	
NURGLE: Exacerbating Resource Consumption in Blockchain State Storage via MPT Manipulation.....	2180
<i>Zheyuan He (University of Electronic Science and Technology of China, China), Zihao Li (The Hong Kong Polytechnic University, China), Ao Qiao (University of Electronic Science and Technology of China, China), Xiapu Luo (The Hong Kong Polytechnic University, China), Xiaosong Zhang (University of Electronic Science and Technology of China, China), Ting Chen (University of Electronic Science and Technology of China, China), Shuwei Song (University of Electronic Science and Technology of China, China), Dijun Liu (Ant Group), and Weina Niu (University of Electronic Science and Technology of China, China)</i>	

Nyx: Detecting Exploitable Front-Running Vulnerabilities in Smart Contracts	2198
<i>Wuqi Zhang (The Hong Kong University of Science and Technology, China), Zhuo Zhang (Purdue University, USA), Qingkai Shi (Purdue University, USA), Lu Liu (The Hong Kong University of Science and Technology, China), Lili Wei (McGill University, Canada), Yepang Liu (Southern University of Science and Technology, China), Xiangyu Zhang (Purdue University, USA), and Shing-Chi Cheung (The Hong Kong University of Science and Technology, China)</i>	
SMARTINV: Multimodal Learning for Smart Contract Invariant Inference	2217
<i>Sally Junsong Wang (Columbia University), Kexin Pei (The University of Chicago), and Junfeng Yang (Columbia University)</i>	
Pulling Off The Mask: Forensic Analysis of the Deceptive Creator Wallets Behind Smart Contract Fraud	2236
<i>Mingxuan Yao (Georgia Institute of Technology), Runze Zhang (Georgia Institute of Technology), Haichuan Xu (Georgia Institute of Technology), Shih-Huan Chou (Georgia Institute of Technology), Varun Chowdhary Paturi (Georgia Institute of Technology), Amit Kumar Sikder (Georgia Institute of Technology), and Brendan Saltaformaggio (Georgia Institute of Technology)</i>	
Towards Smart Contract Fuzzing on GPU	2255
<i>Weimin Chen (The Hong Kong Polytechnic University), Xiapu Luo (The Hong Kong Polytechnic University), Haipeng Cai (Washington State University), and Haoyu Wang (Huazhong University of Science and Technology)</i>	
Large-Scale Study of Vulnerability Scanners for Ethereum Smart Contracts	2273
<i>Christoph Sendner (University of Würzburg, Germany), Lukas Petzi (University of Würzburg, Germany), Jasper Stang (University of Würzburg, Germany), and Alexandra Dmitrienko (University of Würzburg, Germany)</i>	

Track 1 - Session 7: IoT Security

Who Left the Door Open? Investigating the Causes of Exposed IoT Devices in an Academic Network	2291
<i>Takayuki Sasaki (Yokohama National University), Takaya Noma (Yokohama National University), Yudai Morii (Yokohama National University), Toshiya Shimura (Yokohama National University), Michel van Eeten (TU Delft/Yokohama National University), Katsunari Yoshioka (Yokohama National University), and Tsutomu Matsumoto (Yokohama National University)</i>	
SyzTrust: State-aware Fuzzing on Trusted OS Designed for IoT Devices	2310
<i>Qinying Wang (Zhejiang University, China; EPFL, Switzerland), Boyu Chang (Zhejiang University, China), Shouling Ji (Zhejiang University, China), Yuan Tian (University of California, Los Angeles, United States), Xuhong Zhang (Zhejiang University, China), Binbin Zhao (Georgia Institute of Technology, United States), Gaoning Pan (Zhejiang University, China), Chenyang Lyu (Zhejiang University, China), Mathias Payer (EPFL, Switzerland), Wenhai Wang (Zhejiang University, China), and Raheem Beyah (Georgia Institute of Technology, United States)</i>	

A Systematic Study of Physical Sensor Attack Hardness	2328
<i>Hyungsub Kim (Purdue University), Rwitam Bandyopadhyay (Purdue University), Muslum Ozgur Ozmen (Purdue University), Z. Berkay Celik (Purdue University), Antonio Bianchi (Purdue University), Yongdae Kim (KAIST), and Dongyan Xu (Purdue University)</i>	
Revisiting Automotive Attack Surfaces: a Practitioners' Perspective	2348
<i>Pengfei Jing (The Hong Kong Polytechnic University, HK), Zhiqiang Cai (Tencent Keen Security Lab, China), Yingjie Cao (The Hong Kong Polytechnic University, HK), Le Yu (The Hong Kong Polytechnic University, HK), Yuefeng Du (Tencent Keen Security Lab, China), Wenkai Zhang (Tencent Keen Security Lab, China), Chenxiong Qian (University of Hong Kong, HK), Xiapu Luo (The Hong Kong Polytechnic University, HK), Sen Nie (Tencent Keen Security Lab, China), and Shi Wu (Tencent Keen Security Lab, China)</i>	
From Virtual Touch to Tesla Command: Unlocking Unauthenticated Control Chains From Smart Glasses for Vehicle Takeover	2366
<i>Xingli Zhang (University of Louisiana at Lafayette, USA), Yazhou Tu (Auburn University, USA), Yan Long (University of Michigan, USA), Liqun Shan (University of Louisiana at Lafayette, USA; University of Pennsylvania, USA), Mohamed A Elsaadani (University of Louisiana at Lafayette, USA), Kevin Fu (Northeastern University, USA), Zhiqiang Lin (The Ohio State University, USA), and Xiali Hei (University of Louisiana at Lafayette, USA; University of Pennsylvania, USA)</i>	
MQTTactic: Security Analysis and Verification for Logic Flaws in MQTT Implementations	2385
<i>Bin Yuan (Huazhong University of Science and Technology, China), Zhanxiang Song (Huazhong University of Science and Technology, China), Yan Jia (Nankai University, China), Zhenyu Lu (Huazhong University of Science and Technology, China), Deqing Zou (Huazhong University of Science and Technology, China), Hai Jin (Huazhong University of Science and Technology, China), and Luyi Xing (Indiana University Bloomington, United States of America)</i>	
Wear's my Data? Understanding the Cross-Device Runtime Permission Model in Wearables	2404
<i>Doguhan Yeke (Purdue University, USA), Muhammad Ibrahim (Purdue University, USA), Güliz Seray Tuncay (Google, USA), Habiba Farrukh (University of California Irvine, USA), Abdullah Imran (Purdue University, USA), Antonio Bianchi (Purdue University, USA), and Z. Berkay Celik (Purdue University, USA)</i>	
Video-Based Cryptanalysis: Extracting Cryptographic Keys from Video Footage of a Device's Power LED Captured by Standard Video Cameras	2422
<i>Ben Nassi (Cornell Tech), Etay Iluz (Ben-Gurion University of the Negev), Or Cohen (Ben-Gurion University of the Negev), Ofek Vayner (Ben-Gurion University of the Negev), Dudi Nassi (Ben-Gurion University of the Negev), Boris Zadov (Ben-Gurion University of the Negev), and Yuval Elovici (Ben-Gurion University of the Negev)</i>	

Track 2 - Session 7: ML Defenses I

SoK: Explainable Machine Learning in Adversarial Environments	2441
<i>Maximilian Noppel (Karlsruhe Institute of Technology, Germany) and Christian Wressnegger (Karlsruhe Institute of Technology, Germany)</i>	
GrOVe: Ownership Verification of Graph Neural Networks using Embeddings	2460
<i>Asim Waheed (University of Waterloo), Vasisht Duddu (University of Waterloo), and N. Asokan (University of Waterloo and Aalto University)</i>	
Revisiting Black-box Ownership Verification for Graph Neural Networks	2478
<i>Ruikai Zhou (University of Utah, USA), Kang Yang (University of Utah, USA), Xiuling Wang (Stevens Insitute of Technology, USA), Wendy Hui Wang (Stevens Insitute of Technology, USA), and Jun Xu (University of Utah, USA)</i>	
CoreLocker: Neuron-level Usage Control	2497
<i>Zihan Wang (The University of Queensland and CSIRO's Data61, Australia), Zhongkui Ma (The University of Queensland, Australia), Xinguo Feng (The University of Queensland, Australia), Ruoxi Sun (CSIRO's Data61, Australia), Hu Wang (The University of Adelaide, Australia), Minhui Xue (CSIRO's Data61, Australia), and Guangdong Bai (The University of Queensland, Australia)</i>	
MEA-Defender: A Robust Watermark against Model Extraction Attack	2515
<i>Peizhuo Lv (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Hualong Ma (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Jiachen Zhou (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Shengzhi Zhang (Department of Computer Science, Metropolitan College, Boston University, USA), Ruigang Liang (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Shenchen Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), Pan Li (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China), and Yingjun Zhang (Institute of Software, Chinese Academy of Sciences, China)</i>	
Securing Graph Neural Networks in MLaaS: A Comprehensive Realisation of Query-based Integrity Verification	2534
<i>Bang Wu (CSIRO's Data61/Monash University), Xingliang Yuan (Monash University), Shuo Wang (Shanghai Jiao Tong University), Qi Li (Tsinghua University), Minhui Xue (CSIRO's Data61), and Shirui Pan (Griffith University)</i>	

SOPHON: Non-Fine-Tunable Learning to Restrain Task Transferability For Pre-trained Models ..	2553
<i>Jiangyi Deng (Zhejiang University, China), Shengyuan Pang (Zhejiang University, China), Yanjiao Chen (Zhejiang University, China), Liangming Xia (Zhejiang University, China), Yijie Bai (Zhejiang University, China), Haiqin Weng (Ant Group, China), and Wenyuan Xu (Zhejiang University, China)</i>	
FLShield: A Validation Based Federated Learning Framework to Defend Against Poisoning Attacks	2572
<i>Ehsanul Kabir (Penn State University), Zeyu Song (Penn State University), Md Rafi Ur Rashid (Penn State University), and Shagufta Mehnaz (Penn State University)</i>	

Track 3 - Session 7: Crypto for Messaging and Storage

Secure Messaging with Strong Compromise Resilience, Temporal Privacy, and Immediate Decryption	2591
<i>Cas Cremers (CISPA Helmholtz Center for Information Security, Germany) and Mang Zhao (CISPA Helmholtz Center for Information Security, Germany)</i>	
Private Hierarchical Governance for Encrypted Messaging	2610
<i>Armin Namavari (Cornell Tech), Barry Wang (Cornell University), Sanketh Menda (Cornell Tech), Ben Nassi (Cornell Tech), Nirvan Tyagi (Stanford University and University of Washington), James Grimmelmann (Cornell University), Amy Zhang (University of Washington), and Thomas Ristenpart (Cornell Tech)</i>	
Enforcing End-to-End Security for Remote Conferencing	2630
<i>Yuelin Liu (ShanghaiTech University, China), Huangxun Chen (Hong Kong University of Science and Technology (Guangzhou), China), and Zhice Yang (ShanghaiTech University, China)</i>	
Injection Attacks Against End-to-End Encrypted Applications	2648
<i>Andrés Fábrega (Cornell University), Carolina Ortega Pérez (Cornell University), Armin Namavari (Cornell University), Ben Nassi (Cornell Tech), Rachit Agarwal (Cornell University), and Thomas Ristenpart (Cornell Tech)</i>	
Device-Oriented Group Messaging: A Formal Cryptographic Analysis of Matrix' Core	2666
<i>Martin Albrecht (King's College London, UK), Benjamin Dowling (University of Sheffield, UK), and Daniel Jones (Royal Holloway, University of London, UK)</i>	
Multi-stage Group Key Distribution and PAKEs: Securing Zoom Groups against Malicious Servers without New Security Elements	2686
<i>Cas Cremers (CISPA Helmholtz Center for Information Security, Germany), Eyal Ronen (Tel Aviv University, Israel), and Mang Zhao (CISPA Helmholtz Center for Information Security, Germany)</i>	
Holepunch: Fast, Secure File Deletion with Crash Consistency	2705
<i>Zachary Ratliff (Harvard), Wittmann Goh (Harvard), Abe Wieland (Harvard), James Mickens (Harvard), and Ryan Williams (Northeastern University)</i>	

INVISILINE: Invisible Plausibly-Deniable Storage	2722
<i>Sandeep Kiran Pinjala (Stony Brook University), Bogdan Carbutar (Florida International University), Anrin Chakraborti (University of Illinois Chicago), and Radu Sion (Stony Brook University)</i>	

Track 1 - Session 8: Wireless Security and Privacy

Guessing on Dominant Paths: Understanding the Limitation of Wireless Authentication Using Channel State Information	2740
<i>Zhe Qu (Central South University), Rui Duan (University of South Florida), Xiao Han (University of South Florida), Shangqing Zhao (University of Oklahoma), Yao Liu (University of South Florida), and Zhuo Lu (University of South Florida)</i>	
MetaFly: Wireless Backhaul Interception via Aerial Wavefront Manipulation	2759
<i>Zhambyl Shaikhanov (Rice University, USA), Sherif Badran (Northeastern University, USA), Hichem Guerboukha (Brown University, USA), Josep Jornet (Northeastern University, USA), Daniel Mittleman (Brown University, USA), and Edward Knightly (Rice University, USA)</i>	
NFCEraser: A Security Threat of NFC Message Modification Caused by Quartz Crystal Oscillator	2775
<i>Jianshuo Liu (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Hong Li (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Mengjie Sun (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Haining Wang (Virginia Tech, USA), Hui Wen (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Zhi Li (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), and Limin Sun (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China)</i>	
Secure Ranging with IEEE 802.15.4z HRP UWB	2794
<i>Xiliang Luo (Apple, USA), Cem Kalkanli (Apple, USA), Hao Zhou (Apple, USA), Pengcheng Zhan (Apple, USA), and Moche Cohen (Apple, USA)</i>	
mimoCrypt: Multi-User Privacy-Preserving Wi-Fi Sensing via MIMO Encryption	2812
<i>Jun Luo (Nanyang Technological University), Hangcheng Cao (Hunan University), Hongbo Jiang (Hunan University), Yanbing Yang (Sichuan University), and Zhe Chen (Fudan University)</i>	
Surveilling the Masses with Wi-Fi-Based Positioning Systems	2831
<i>Erik Rye (University of Maryland, USA) and Dave Levin (University of Maryland, USA)</i>	

SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth	2847
<i>Jianliang Wu (Purdue University & Simon Fraser University), Ruoyu Wu (Purdue University), Dongyan Xu (Purdue University), Dave Tian (Purdue University), and Antonio Bianchi (Purdue University)</i>	
Practical Obfuscation of BLE Physical-Layer Fingerprints on Mobile Devices	2867
<i>Hadi Givvehchian (UC San Diego), Nishant Bhaskar (UC San Diego), Alexander Redding (UC San Diego), Han Zhao (UC San Diego), Aaron Schulman (UC San Diego), and Dinesh Bharadia (UC San Diego)</i>	

Track 2 - Session 8: ML Defenses II

It's Simplex! Disaggregating Measures to Improve Certified Robustness	2886
<i>Andrew C. Cullen (University of Melbourne, Australia), Paul Montague (Defence Science and Technology Group, Australia), Shijie Liu (University of Melbourne, Australia), Sarah M. Erfani (University of Melbourne, Australia), and Benjamin I.P. Rubinstein (University of Melbourne, Australia)</i>	
Sabre: Cutting through Adversarial Noise with Adaptive Spectral Filtering and Input Reconstruction	2901
<i>Alec F. Diallo (The University of Edinburgh, UK) and Paul Patras (The University of Edinburgh, UK)</i>	
Text-CRS: A Generalized Certified Robustness Framework against Textual Adversarial Attacks...	2920
<i>Xinyu Zhang (Zhejiang University, China; University of Connecticut, USA), Hanbin Hong (University of Connecticut, USA), Yuan Hong (University of Connecticut, USA), Peng Huang (Zhejiang University, China), Binghui Wang (Illinois Institute of Technology, USA), Zhongjie Ba (Zhejiang University, China), and Kui Ren (Zhejiang University, China)</i>	
FCert: Certifiably Robust Few-Shot Classification in the Era of Foundation Models	2939
<i>Yanting Wang (The Pennsylvania State University, USA), Wei Zou (The Pennsylvania State University, USA), and Jinyuan Jia (The Pennsylvania State University, USA)</i>	
Node-aware Bi-smoothing: Certified Robustness against Graph Injection Attacks	2958
<i>Yuni Lai (The Hong Kong Polytechnic University), Yulin Zhu (The Hong Kong Polytechnic University), Bailin Pan (The Hong Kong Polytechnic University), and Kai Zhou (The Hong Kong Polytechnic University)</i>	
LACMUS: Latent Concept Masking for General Robustness Enhancement of DNNs	2977
<i>Shuo Wang (Shanghai Jiao Tong University, China), Hongsheng Hu (CSIRO's Data61, Australia), Jiamin Chang (University of New South Wales and CSIRO's Data61, Australia), Benjamin Zi Hao Zhao (Macquarie University), and Minhui Xue (CSIRO's Data61, Australia)</i>	
SoK: Unintended Interactions among Machine Learning Defenses and Risks	2996
<i>Vasisht Duddu (University of Waterloo), Sebastian Szyller (Intel Labs), and N. Asokan (University of Waterloo, Aalto University)</i>	

Securely Fine-tuning Pre-trained Encoders Against Adversarial Examples	3015
<i>Ziqi Zhou (Huazhong University of Science and Technology), Minghui Li (Huazhong University of Science and Technology), Wei Liu (Huazhong University of Science and Technology), Shengshan Hu (Huazhong University of Science and Technology), Yechao Zhang (Huazhong University of Science and Technology), Wei Wan (Huazhong University of Science and Technology), Lulu Xue (Huazhong University of Science and Technology), Leo Yu Zhang (Griffith University), Dezhong Yao (Huazhong University of Science and Technology), and Hai Jin (Huazhong University of Science and Technology)</i>	

Track 3 - Session 8: Crypto

hinTS: Threshold Signatures with Silent Setup	3034
<i>Sarjam Garg (UC Berkeley and NTT Research), Abhishek Jain (JHU and NTT Research), Pratyay Mukherjee (Supra Research), Rohit Sinha (Swirls Labs), Mingyuan Wang (UC Berkeley), and Yinuo Zhang (UC Berkeley)</i>	
Threshold ECDSA in Three Rounds	3053
<i>Jack Doerner (Technion, Israel; Reichman University, Israel; Brown University, USA), Yashwanth Kondi (Silence Laboratories (Deel), USA), Eysa Lee (Brown University, USA), and abhi shelat (Northeastern University, USA)</i>	
Private Analytics via Streaming, Sketching, and Silently Verifiable Proofs	3072
<i>Mayank Rathee (University of California, Berkeley), Yuwen Zhang (University of California, Berkeley), Henry Corrigan-Gibbs (Massachusetts Institute of Technology), and Raluca Ada Popa (University of California, Berkeley)</i>	
Hyena: Balancing Packing, Reuse, and Rotations for Encrypted Inference	3091
<i>Sarabjeet Singh (University of Utah), Shreyas Singh (University of Utah), Sumanth Gudaparthi (University of Utah), Xiong Fan (Rutgers University), and Rajeev Balasubramonian (University of Utah)</i>	
Make Revocation Cheaper: Hardware-Based Revocable Attribute-Based Encryption	3109
<i>Xiaoguo Li (Singapore Management University, Singapore), Guomin Yang (Singapore Management University, Singapore), Tao Xiang (Chongqing University, China), Shengmin Xu (Fujian Normal University, China), Bowen Zhao (Guangzhou Institute of Technology, Xidian University, China), HweeHwa Pang (Singapore Management University, Singapore), and Robert H. Deng (Singapore Management University, Singapore)</i>	
SoK: Efficient Design and Implementation of Polynomial Hash Functions over Prime Fields	3128
<i>Jean Paul Degabriele (Technology Innovation Institute, United Arab Emirates), Jan Gilcher (ETH Zurich, Switzerland), Jérôme Govinden (TU Darmstadt, Germany), and Kenneth G. Paterson (ETH Zurich, Switzerland)</i>	
Springproofs: Efficient Inner Product Arguments for Vectors of Arbitrary Length	3147
<i>Jianning Zhang (College of Computer Science & Cyber Science, Nankai University, Tianjin, China), Ming Su (College of Computer Science & Cyber Science, Nankai University, Tianjin, China), Xiaoguang Liu (College of Computer Science & Cyber Science, Nankai University, Tianjin, China), and Gang Wang (College of Computer Science & Cyber Science, Nankai University, Tianjin, China)</i>	

CryptoVampire: Automated Reasoning for the Complete Symbolic Attacker Cryptographic Model 3165

Simon Jeanteur (TU Wien), Laura Kovács (TU Wien), Matteo Maffei (TU Wien), and Michael Rawson (TU Wien)

Track 1 - Session 9: Applications of Privacy

Nebula: A Privacy-First Platform for Data Backhaul 3184

Jean-Luc Watson (University of California, Berkeley), Tess Despres (University of California, Berkeley), Alvin Tan (University of California, Berkeley), Shishir G Patil (University of California, Berkeley), Prabal Dutta (University of California, Berkeley), and Raluca Ada Popa (University of California, Berkeley)

Pudding: Private User Discovery in Anonymity Networks 3203

Ceren Kocaogullar (University of Cambridge, United Kingdom), Daniel Hugenroth (University of Cambridge, United Kingdom), Martin Kleppmann (TU Munich, Germany), and Alastair R. Beresford (University of Cambridge, United Kingdom)

Attacking and Improving the Tor Directory Protocol 3221

Zhongtang Luo (Purdue University), Adithya Bhat (Purdue University), Kartik Nayak (Duke University), and Aniket Kate (Purdue University / Supra Research)

Real-Time Website Fingerprinting Defense via Traffic Cluster Anonymization 3238

Meng Shen (Beijing Institute of Technology, China), Kexin Ji (Beijing Institute of Technology, China), Jinhe Wu (Beijing Institute of Technology, China), Qi Li (Tsinghua University, China), Xiangdong Kong (Beijing Institute of Technology, China), Ke Xu (Tsinghua University, China), and Liehuang Zhu (Beijing Institute of Technology, China)

Learn What You Want to Unlearn: Unlearning Inversion Attacks against Machine Unlearning 3257

Hongsheng Hu (CSIRO's Data61, Australia), Shuo Wang (Shanghai Jiao Tong University, China), Tian Dong (Shanghai Jiao Tong University, China), and Minhui Xue (CSIRO's Data61)

Few-shot Unlearning 3276

Youngsik Yoon (Pohang University of Science and Technology), Jinhwan Nam (Pohang University of Science and Technology), Hyojeong Yun (Pohang University of Science and Technology), Jaeho Lee (Pohang University of Science and Technology), Dongwoo Kim (Pohang University of Science and Technology), and Jungseul Ok (Pohang University of Science and Technology)

Track 2 - Session 9: Miscellaneous ML

DeepShuffle: A Lightweight Defense Framework against Adversarial Fault Injection Attacks on Deep Neural Networks in Multi-tenant Cloud-FPGA 3293

Yukui Luo (Northeastern University), Adnan Siraj Rakin (Binghamton University), Deliang Fan (Johns Hopkins University), and Xiaolin Xu (Northeastern University)

DeepTheft: Stealing DNN Model Architectures through Power Side Channel	3311
<i>Yansong Gao (CSIRO's Data61), Huming Qiu (Fudan University), Zhi Zhang (The University of Western Australia), Binghui Wang (The University of Western Australia), Hua Ma (The University of Adelaide), Alsharif Abuadbbba (CSIRO's Data61), Minhui Xue (CSIRO's Data61), Anmin Fu (Nanjing University of Science and Technology), and Surya Nepal (CSIRO's Data61)</i>	
No Privacy Left Outside: On the (In-)Security of TEE-Shielded DNN Partition for On-Device ML	3327
<i>Ziqi Zhang (Peking University), Chen Gong (Peking University), Yifeng Cai (Peking University), Yuanyuan Yuan (HKUST), Bingyan Liu (Peking University), Ding Li (Peking University), Yao Guo (Peking University), and Xiangqun Chen (Peking University)</i>	
One for All and All for One: GNN-based Control-Flow Attestation for Embedded Devices	3346
<i>Marco Chilese (Technical University Darmstadt, Germany), Richard Mitev (Technical University Darmstadt, Germany), Meni Orenbach (NVIDIA), Robert Thorburn (University of Southampton), Ahmad Atamli (NVIDIA, University of Southampton), and Ahmad-Reza Sadeghi (Technical University Darmstadt, Germany)</i>	
Why Does Little Robustness Help? A Further Step Towards Understanding Adversarial Transferability	3365
<i>Yechao Zhang (Huazhong University of Science and Technology), Shengshan Hu (Huazhong University of Science and Technology), Leo Yu Zhang (Griffith University), Junyu Shi (Huazhong University of Science and Technology), Minghui Li (Huazhong University of Science and Technology), Xiaogeng Liu (Huazhong University of Science and Technology), Wei Wan (Huazhong University of Science and Technology), and Hai Jin (Huazhong University of Science and Technology)</i>	
Backdooring Multimodal Learning	3385
<i>Xingshuo Han (Nanyang Technological University, Singapore), Yutong Wu (Nanyang Technological University, Singapore), Qingjie Zhang (Shanghai Jiao Tong University, China), Yuan Zhou (Nanyang Technological University, Singapore), Yuan Xu (Nanyang Technological University, Singapore), Han Qiu (Tsinghua University, China), Guowen Xu (Nanyang Technological University, Singapore), and Tianwei Zhang (Nanyang Technological University, Singapore)</i>	

Track 3 - Session 9: Security for Democracy

Understanding the Privacy Practices of Political Campaigns: A Perspective from the 2020 US Election Websites	3404
<i>Kaushal Kafle (William & Mary, USA), Prianka Mandal (William & Mary, USA), Kapil Singh (IBM T.J. Watson Research Center, USA), Benjamin Andow (Google, USA), and Adwait Nadkarni (William & Mary, USA)</i>	
Thwarting Last-Minute Voter Coercion	3423
<i>Rosario Giustolisi (IT University of Copenhagen, Denmark), Maryam Sheikhi Garjan (IT University of Copenhagen, Denmark), and Carsten Schuermann (IT University of Copenhagen, Denmark)</i>	

Can we cast a ballot as intended and be receipt free?	3440
<i>Henri Devillez (UCLouvain, Belgium), Olivier Pereira (UCLouvain, Belgium; Microsoft Research, USA), Thomas Peters (UCLouvain, Belgium), and Quentin Yang (Université de Lorraine, France)</i>	
Investigating Voter Perceptions of Printed Physical Audit Trails for Online Voting	3458
<i>Karola Marky (Ruhr University Bochum), Nina Gerber (Technical University of Darmstadt), Henry John Krumb (Technical University of Darmstadt), Mohamed Khamis (University of Glasgow), and Max Mühlhäuser (Technical University of Darmstadt)</i>	
E-Vote Your Conscience: Perceptions of Coercion and Vote Buying, and the Usability of Fake Credentials in Online Voting	3478
<i>Louis-Henri Merino (EPFL, Switzerland), Alaleh Azhir (MIT, United States), Haoqian Zhang (EPFL, Switzerland), Simone Colombo (EPFL, Switzerland), Bernhard Tellenbach (Armasuisse, Switzerland), Vero Estrada-Galiñanes (EPFL, Switzerland), and Bryan Ford (EPFL, Switzerland)</i>	
NetShuffle: Circumventing Censorship with Shuffle Proxies at the Edge	3497
<i>Patrick Tser Jern Kon (Rice University, USA), Aniket Gattani (Rice University, USA), Dhiraj Saharia (Georgetown University, USA), Tianyu Cao (Rice University, USA), Diogo Barradas (University of Waterloo, Canada), Ang Chen (University of Michigan, USA), Micah Sherr (Georgetown University, USA), and Benjamin E. Ujcich (Georgetown University, USA)</i>	

Track 1 - Session 10: Provenance and Enterprise Security

R-CAID: Embedding Root Cause Analysis within Provenance-based Intrusion Detection	3515
<i>Akul Goyal (University of Illinois Urbana Champaign), Gang Wang (University of Illinois Urbana Champaign), and Adam Bates (University of Illinois Urbana Champaign)</i>	
KAIROS: Practical Intrusion Detection and Investigation using Whole-system Provenance	3533
<i>Zijun Cheng (University of Chinese Academy of Sciences, China), Qiujian Lv (Chinese Academy of Sciences, China), Jinyuan Liang (University of British Columbia, Canada), Yan Wang (Chinese Academy of Sciences, China), Degang Sun (Chinese Academy of Sciences, China), Thomas Pasquier (University of British Columbia, Canada), and Xueyuan Han (Wake Forest University)</i>	
FLASH: A Comprehensive Approach to Intrusion Detection via Provenance Graph Representation Learning	3552
<i>Mati Ur Rehman (University of Virginia, USA), Hadi Ahmadi (Corvic Inc, USA), and Wajih Ul Hassan (University of Virginia, USA)</i>	
eAUDIT: A Fast, Scalable and Deployable Audit Data Collection System	3571
<i>R. Sekar (Stony Brook University, USA), Hanke Kimm (Stony Brook University, USA), and Rohit Aich (Stony Brook University, USA)</i>	
Understanding and Bridging the Gap Between Unsupervised Network Representation Learning and Security Analytics	3590
<i>Jiacen Xu (University of California, Irvine), Xiaokui Shu (IBM Research), and Zhou Li (University of California, Irvine)</i>	

DrSec: Flexible Distributed Representations for Efficient Endpoint Security	3609
<i>Mahmood Sharif (Tel Aviv University, Israel), Pubali Datta (University of Massachusetts Amherst, USA), Andy Riddle (University of Illinois Urbana-Champaign, USA), Kim Westfall (University of Illinois Urbana-Champaign, USA), Adam Bates (University of Illinois Urbana-Champaign, USA), Vijay Ganti (Google, USA), Matthew Lentz (Duke University, USA), and David Ott (VMware, USA)</i>	

Do You Play It by the Books? A Study on Incident Response Playbooks and Influencing Factors	3625
<i>Daniel Schlette (University of Regensburg, Germany), Philip Empl (University of Regensburg, Germany), Marco Caselli (Siemens AG, Germany), Thomas Schreck (HM Munich University of Applied Sciences, Germany), and Günther Pernul (University of Regensburg, Germany)</i>	

Jbeil: Temporal Graph-Based Inductive Learning to Infer Lateral Movement in Evolving Enterprise Networks	3644
<i>Joseph Khoury (Louisiana State University, USA), Đorđe Klisura (Louisiana State University, USA), Hadi Zanddizari (The University of Texas at San Antonio, USA), Gonzalo De La Torre Parra (The University of the Incarnate Word, USA), Peyman Najafirad (The University of Texas at San Antonio, USA), and Elias Bou-Harb (Louisiana State University, USA)</i>	

Track 2 - Session 10: Hardware Sidechannels

Efficient and Generic Microarchitectural Hash-Function Recovery	3661
<i>Lukas Gerlach (CISPA Helmholtz Center for Information Security), Simon Schwarz (Saarland University, Saarland Informatics Campus), Nicolas Faröß (Saarland University, Department of Mathematics), and Michael Schwarz (CISPA Helmholtz Center for Information Security)</i>	

BUSTed!!! Microarchitectural Side-Channel Attacks on the MCU Bus Interconnect	3679
<i>Cristiano Rodrigues (Universidade do Minho), Daniel Oliveira (Universidade do Minho), and Sandro Pinto (Universidade do Minho)</i>	

Architectural Mimicry: Innovative Instructions to Efficiently Address Control-Flow Leakage in Data-Oblivious Programs	3697
<i>Hans Winderix (KU Leuven, Belgium), Marton Bognar (KU Leuven, Belgium), Job Noorman (KU Leuven, Belgium), Lesly-Ann Daniel (KU Leuven, Belgium), and Frank Piessens (KU Leuven, Belgium)</i>	

GPU.zip: On the Side-Channel Implications of Hardware-Based Graphical Data Compression	3716
<i>Yingchen Wang (The University of Texas at Austin), Riccardo Paccagnella (Carnegie Mellon University), Zhao Gang (The University of Texas at Austin), Willy Vasquez (The University of Texas at Austin), David Kohlbrenner (University of Washington), Hovav Shacham (The University of Texas at Austin), and Christopher Fletcher (University of Illinois Urbana-Champaign)</i>	

CONJUNCT: Learning Inductive Invariants to Prove Unbounded Instruction Safety Against Microarchitectural Timing Attacks	3735
<i>Sushant Dinesh (University of Illinois Urbana-Champaign), Madhusudan Parthasarathy (University of Illinois Urbana-Champaign), and Christopher Fletcher (University of Illinois Urbana-Champaign)</i>	

Prune+PlumTree - Finding Eviction Sets at Scale	3754
<i>Tom Kessous (Ben-Gurion University of the Negev, Israel) and Niv Gilboa (Ben-Gurion University of the Negev, Israel)</i>	
Leaky Address Masking: Exploiting Unmasked Spectre Gadgets with Noncanonical Address Translation	3773
<i>Mathé Hertogh (Vrije Universiteit Amsterdam, The Netherlands), Sander Wiebing (Vrije Universiteit Amsterdam, The Netherlands), and Cristiano Giuffrida (Vrije Universiteit Amsterdam, The Netherlands)</i>	
Rethinking IC Layout Vulnerability: Simulation-Based Hardware Trojan Threat Assessment with High Fidelity	3789
<i>Xinming Wei (Peking University, China), Jiaxi Zhang (Peking University, China), and Guojie Luo (Peking University, China)</i>	

Track 3 - Session 10: Blockchain II

Routing Attacks on Cryptocurrency Mining Pools	3805
<i>Muoi Tran (ETH Zurich, Switzerland), Theo von Arx (ETH Zurich, Switzerland), and Laurent Vanbever (ETH Zurich, Switzerland)</i>	
Sweep-UC: Swapping Coins Privately	3822
<i>Lucjan Hanzlik (CISPA Helmholtz Center for Information Security), Julian Loss (CISPA Helmholtz Center for Information Security), Sri AravindaKrishnan Thyagarajan (NTT Research), and Benedikt Wagner (CISPA Helmholtz Center for Information Security & Saarland University)</i>	
SoK: Security and Privacy of Blockchain Interoperability	3840
<i>André Augusto (INESC-ID & Instituto Superior Técnico, Portugal), Rafael Belchior (INESC-ID & Instituto Superior Técnico, Portugal), Miguel Correia (INESC-ID & Instituto Superior Técnico, Portugal), André Vasconcelos (INESC-ID & Instituto Superior Técnico, Portugal), Luyao Zhang (Duke Kunshan University, China), and Thomas Hardjono (MIT Connection Science, USA)</i>	
Non-Atomic Arbitrage in Decentralized Finance	3866
<i>Lioba Heimbach (ETH Zurich), Vabuk Pahari (MPI-SWS), and Eric Schertenleib (unaffiliated)</i>	
Optimal Flexible Consensus and its Application to Ethereum	3885
<i>Joachim Neu (Stanford University, USA), Srivatsan Sridhar (Stanford University, USA), Lei Yang (Massachusetts Institute of Technology, USA), and David Tse (Stanford University, USA)</i>	
PriDe CT: Towards Public Consensus, Private Transactions, and Forward Secrecy in Decentralized Payments	3904
<i>Yue Guo (J.P. Morgan AI Research, J.P. Morgan AlgoCRYPT CoE), Harish Karthikeyan (J.P. Morgan AI Research, J.P. Morgan AlgoCRYPT CoE), Antigoni Polychoriadou (J.P. Morgan AI Research, J.P. Morgan AlgoCRYPT CoE), and Chaddy Huussin (J.P. Morgan Chase & Co.)</i>	
POMABuster: Detecting Price Oracle Manipulation Attacks in Decentralized Finance	3923
<i>Rui Xi (University of British Columbia, Canada), Zehua Wang (University of British Columbia, Canada), and Karthik Pattabiraman (University of British Columbia, Canada)</i>	

Specular: Towards Secure, Trust-minimized Optimistic Blockchain Execution	3943
<i>Zhe Ye (University of California, Berkeley, USA), Ujval Misra (University of California, Berkeley, USA), Jiajun Cheng (ShanghaiTech University, China), Wenyang Zhou (University of Cambridge, UK), and Dawn Song (University of California, Berkeley, USA)</i>	

Track 1 - Session 11: Software Analysis

Efficient Detection of Java Deserialization Gadget Chains via Bottom-up Gadget Search and Dataflow-aided Payload Construction	3961
<i>Bofei Chen (Fudan University), Lei Zhang (Fudan University, China), Xinyou Huang (Fudan University, China), Yinzhi Cao (Johns Hopkins University), Keke Lian (Fudan University, China), Yuan Zhang (Fudan University, China), and Min Yang (Fudan University, China)</i>	
"False negative - that one is going to kill you." - Understanding Industry Perspectives of Static Analysis based Security Testing	3979
<i>Amit Seal Ami (William & Mary, USA), Kevin Moran (University of Central Florida, USA), Denys Poshyvanyk (William & Mary, USA), and Adwait Nadkarni (William & Mary, USA)</i>	
AirTaint: Making Dynamic Taint Analysis Faster and Easier	3998
<i>Qian Sang (University of Chinese Academy of Sciences, China), Yanhao Wang (Institute of Software Chinese Academy of Sciences, China), Yuwei Liu (University of Chinese Academy of Sciences, China), Xiangkun Jia (Institute of Software Chinese Academy of Sciences, China), Tiffany Bao (Arizona State University), and Purui Su (Institute of Software Chinese Academy of Sciences, China)</i>	
Undefined-oriented Programming: Detecting and Chaining Prototype Pollution Gadgets in Node.js Template Engines for Malicious Consequences	4015
<i>Zhengyu Liu (Johns Hopkins University), Kecheng An (Johns Hopkins University), and Yinzhi Cao (Johns Hopkins University)</i>	
APP-Miner: Detecting API Misuses via Automatically Mining API Path Patterns	4034
<i>Jiasheng Jiang (Institute of Software, Chinese Academy of Sciences, China), Jingzheng Wu (Institute of Software, Chinese Academy of Sciences, China), Xiang Ling (Institute of Software, Chinese Academy of Sciences, China), Tianyue Luo (Institute of Software, Chinese Academy of Sciences, China), Sheng Qu (Institute of Software, Chinese Academy of Sciences, China), and Yanjun Wu (Institute of Software, Chinese Academy of Sciences, China)</i>	
ERASAN : Efficient Rust Address Sanitizer	4053
<i>Jiun Min (UNIST), Dongyeon Yu (UNIST), Seongyun Jeong (UNIST), Dokyung Song (Yonsei University), and Yuseok Jeon (UNIST)</i>	

"Len or index or count, anything but v1": Predicting Variable Names in Decompilation Output with Transfer Learning	4069
<i>Kuntal Kumar Pal (Arizona State University, USA), Ati Priya Bajaj (Arizona State University, USA), Pratyay Banerjee (Arizona State University, USA), Audrey Dutcher (Arizona State University, USA), Mutsumi Nakamura (Arizona State University, USA), Zion Leonahenahe Basque (Arizona State University, USA), Himanshu Gupta (Arizona State University, USA), Saurabh Arjun Sawant (Arizona State University, USA), Ujjwala Anantheswaran (Arizona State University, USA), Yan Shoshitaishvili (Arizona State University, USA), Adam Doupe (Arizona State University, USA), Chitta Baral (Arizona State University, USA), and Ruoyu Wang (Arizona State University, USA)</i>	
SrcMarker: Dual-Channel Source Code Watermarking via Scalable Code Transformations	4088
<i>Borui Yang (Shanghai Jiao Tong University), Wei Li (Shanghai Jiao Tong University), Liyao Xiang (Shanghai Jiao Tong University), and Bo Li (Hong Kong University of Science and Technology)</i>	

Track 2 - Session 11: TEE and Hardware Security

UnTrustZone: Systematic Accelerated Aging to Expose On-chip Secrets	4107
<i>Jubayer Mahmud (Virginia Tech, USA) and Matthew Hicks (Virginia Tech, USA)</i>	
On (the Lack of) Code Confidentiality in Trusted Execution Environments	4125
<i>Ivan Puddu (ETH Zurich, Switzerland), Moritz Schneider (ETH Zurich, Switzerland), Daniele Lain (ETH Zurich, Switzerland), Stefano Boschetto (ETH Zurich, Switzerland), and Srdjan Capkun (ETH Zurich, Switzerland)</i>	
SoK: SGX.Fail: How Stuff Gets eXposed	4143
<i>Stephan van Schaik (University of Michigan), Alex Seto (Purdue University), Thomas Yurek (UIUC), Adam Batori (University of Michigan), Bader AlBassam (Purdue University), Daniel Genkin (Georgia Tech), Andrew Miller (UIUC), Eyal Ronen (Tel Aviv University), Yuval Yarom (Ruhr University Bochum), and Christina Garman (Purdue University)</i>	
Pandora: Principled Symbolic Validation of Intel SGX Enclave Runtimes	4163
<i>Fritz Alder (DistriNet, KU Leuven, Belgium), Lesly-Ann Daniel (DistriNet, KU Leuven, Belgium), David Oswald (University of Birmingham, UK), Frank Piessens (DistriNet, KU Leuven, Belgium), and Jo Van Bulck (DistriNet, KU Leuven, Belgium)</i>	
Obelix: Mitigating Side-Channels through Dynamic Obfuscation	4182
<i>Jan Wichelmann (Universität zu Lübeck, Germany), Anja Rabich (Universität zu Lübeck, Germany), Anna Pätschke (Universität zu Lübeck, Germany), and Thomas Eisenbarth (Universität zu Lübeck, Germany)</i>	
Serberus: Protecting Cryptographic Code from Spectres at Compile-Time	4200
<i>Nicholas Mosier (Stanford University), Hamed Nemati (CISPA Helmholtz Center for Information Security), John C. Mitchell (Stanford University), and Caroline Trippel (Stanford University)</i>	

WESEE: Using Malicious #VC Interrupts to Break AMD SEV-SNP	4220
<i>Benedict Schlüter (ETH Zurich, Switzerland), Supraja Sridhara (ETH Zurich, Switzerland), Andrin Bertschi (ETH Zurich, Switzerland), and Shweta Shinde (ETH Zurich, Switzerland)</i>	
Sticky Tags: Efficient and Deterministic Spatial Memory Error Mitigation using Persistent Memory Tags	4239
<i>Floris Gorter (Vrije Universiteit Amsterdam), Taddeus Kroes (Vrije Universiteit Amsterdam), Herbert Bos (Vrije Universiteit Amsterdam), and Cristiano Giuffrida (Vrije Universiteit Amsterdam)</i>	

Track 3 - Session 11: ORAM and PIR

BULKOR: Enabling Bulk Loading for Path ORAM	4258
<i>Xiang Li (Tsinghua University), Yunqian Luo (Tsinghua University), and Mingyu Gao (Tsinghua University)</i>	
Distributed & Scalable Oblivious Sorting and Shuffling	4277
<i>Nicholas Ngai (UC Berkeley), Ioannis Demertzis (UC Santa Cruz), Javad Ghareh Chamani (HKUST), and Dimitrios Papadopoulos (HKUST)</i>	
PIANO: Extremely Simple, Single-Server PIR with Sublinear Server Computation	4296
<i>Mingxun Zhou (Carnegie Mellon University, USA), Andrew Park (Carnegie Mellon University, USA), Wenting Zheng (Carnegie Mellon University, USA), and Elaine Shi (Carnegie Mellon University, USA)</i>	
PIRANA: Faster Multi-query PIR via Constant-weight Codes	4315
<i>Jian Liu (Zhejiang University), Jingyu Li (Zhejiang University), Di Wu (Zhejiang University), and Kui Ren (Zhejiang University)</i>	
Communication-efficient, Fault Tolerant PIR over Erasure Coded Storage	4331
<i>Andrew Park (Carnegie Mellon University), Trevor Leong (Carnegie Mellon University), Francisco Maturana (Carnegie Mellon University), Wenting Zheng (Carnegie Mellon University), and Rashmi Vinayak (Carnegie Mellon University)</i>	
More is Merrier: Relax the Non-Collusion Assumption in Multi-server PIR	4348
<i>Tiantian Gong (Purdue University, USA), Ryan Henry (University of Calgary, Canada), Alexandros Psomas (Purdue University, USA), and Aniket Kate (Purdue University, USA)</i>	
Group Oblivious Message Retrieval	4367
<i>Zeyu Liu (Yale University), Eran Tromer (Boston University), and Yunhao Wang (Yale University)</i>	
PolySphinx: Extending the Sphinx Mix Format With Better Multicast Support	4386
<i>Daniel Schadt (Karlsruhe Institute of Technology, Germany), Christoph Coijanovic (Karlsruhe Institute of Technology, Germany), Christiane Weis (NEC Laboratories, Germany), and Thorsten Strufe (Karlsruhe Institute of Technology, Germany)</i>	

Track 1 - Session 12: Network Security

Where Are the Red Lines? Towards Ethical Server-Side Scans in Security and Privacy Research	4405
<i>Florian Hantke (CISPA Helmholtz Center for Information Security), Sebastian Roth (TU Wien), Rafael Mrowczynski (CISPA Helmholtz Center for Information Security), Christine Utz (CISPA Helmholtz Center for Information Security), and Ben Stock (CISPA Helmholtz Center for Information Security)</i>	
Cerberus: Enabling Efficient and Effective In-Network Monitoring on Programmable Switches ...	4424
<i>Huancheng Zhou (Texas A&M University) and Guofei Gu (Texas A&M University)</i>	
Pryde: A Modular Generalizable Workflow for Uncovering Evasion Attacks Against Stateful Firewall Deployments	4440
<i>Soo-Jin Moon (Carnegie Mellon University, USA), Milind Srivastava (Carnegie Mellon University, USA), Yves Bieri (Compass Security, Switzerland), Ruben Martins (Carnegie Mellon University, USA), and Vyas Sekar (Carnegie Mellon University, USA)</i>	
TUDOOR Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets	4459
<i>Xiang Li (Tsinghua University), Wei Xu (Tsinghua University), Baojun Liu (Tsinghua University), Mingming Zhang (Tsinghua University and Zhongguancun Laboratory), Zhou Li (University of California, Irvine), Jia Zhang (Tsinghua University and Zhongguancun Laboratory), Deliang Chang (QI-ANXIN Technology Research Institute), Xiaofeng Zheng (Tsinghua University and QI-ANXIN Technology Research Institute), Chuhan Wang (Tsinghua University), Jianjun Chen (Tsinghua University and Zhongguancun Laboratory), Haixin Duan (Tsinghua University; Zhongguancun Laboratory; Quan Cheng Laboratory), and Qi Li (Tsinghua University)</i>	
DNSBOMB: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses	4478
<i>Xiang Li (Tsinghua University), Dashuai Wu (Tsinghua University), Haixin Duan (Tsinghua University; Zhongguancun Laboratory; Quan Cheng Laboratory), and Qi Li (Tsinghua University)</i>	
TCP Spoofing: Reliable Payload Transmission Past the Spoofed TCP Handshake	4497
<i>Yepeng Pan (CISPA Helmholtz Center for Information Security, Germany) and Christian Rossow (CISPA Helmholtz Center for Information Security, Germany)</i>	
Practical Attacks Against DNS Reputation Systems	4516
<i>Tillson Galloway (Georgia Institute of Technology), Kleanthis Karakolios (Georgia Institute of Technology), Zane Ma (Oregon State University), Roberto Perdisci (University of Georgia, Georgia Institute of Technology), Angelos Keromytis (Georgia Institute of Technology), and Manos Antonakakis (Georgia Institute of Technology)</i>	
Leveraging Prefix Structure to Detect Volumetric DDoS Attack Signatures with Programmable Switches	4535
<i>Chris Misa (University of Oregon), Ramakrishnan Durairajan (University of Oregon), Arpit Gupta (UCSB), Reza Rejaie (University of Oregon), and Walter Willinger (NIKSUN, Inc.)</i>	

Track 2 - Session 12: Systems Security

Automated Synthesis of Effect Graph Policies for Microservice-Aware Stateful System Call Specialization	4554
<i>William Blair (Boston University), Frederico Araujo (IBM Research), Teryl Taylor (IBM Research), and Jiyong Jang (IBM Research)</i>	
SoK: A Comprehensive Analysis and Evaluation of Docker Container Attack and Defense Mechanisms	4573
<i>Md Sadun Haq (The University Of Texas At San Antonio), Thien Duc Nguyen (Technical University of Darmstadt), Franziska Vollmer (Technical University of Darmstadt), Ali Saman Tosun (University Of North Carolina at Pembroke), Ahmad-Reza Sadeghi (Technical University of Darmstadt), and Turgay Korkmaz (University Of Texas At San Antonio)</i>	
Tabbed Out: Subverting the Android Custom Tab Security Model	4591
<i>Philipp Beer (TU Wien), Marco Squarcina (TU Wien), Lorenzo Veronese (TU Wien), and Martina Lindorfer (TU Wien)</i>	
P4Control: Line-Rate Cross-Host Attack Prevention via In-Network Information Flow Control Enabled by Programmable Switches and eBPF	4610
<i>Osama Bajaber (Virginia Tech), Bo Ji (Virginia Tech), and Peng Gao (Virginia Tech)</i>	
To Boldly Go Where No Fuzzer Has Gone Before: Finding Bugs in Linux' Wireless Stacks through VirtIO Devices	4629
<i>Sönke Huster (Secure Mobile Networking Lab (SEEMOO), TU Darmstadt, Germany; Computer Security and Privacy, University of Göttingen, Germany), Matthias Hollick (Secure Mobile Networking Lab (SEEMOO), TU Darmstadt, Germany), and Jiska Classen (Secure Mobile Networking Lab (SEEMOO), TU Darmstadt, Germany; Hasso Plattner Institute, University of Potsdam, Germany)</i>	
SATURN: Host-Gadget Synergistic USB Driver Fuzzing	4646
<i>Yiru Xu (Tsinghua University, China), Hao Sun (Tsinghua University, China), Jianzhong Liu (Tsinghua University, China), Yuheng Shen (Tsinghua University, China), and Yu Jiang (Tsinghua University, China)</i>	
SyzGen++: Dependency Inference for Augmenting Kernel Driver Fuzzing	4661
<i>Weiteng Chen (Microsoft Research), Yu Hao (University of California, Riverside), Zheng Zhang (University of California, Riverside), Xiaochen Zou (University of California, Riverside), Dhilung Kirat (IBM Research), Shachee Mishra (IBM Research), Douglas Schales (IBM Research), Jiyong Jang (IBM Research), and Zhiyun Qian (University of California, Riverside)</i>	
Side-Channel-Assisted Reverse-Engineering of Encrypted DNN Hardware Accelerator IP and Attack Surface Exploration	4678
<i>Cheng Gongye (Northeastern University, USA), Yukui Luo (Northeastern University, USA), Xiaolin Xu (Northeastern University, USA), and Yunsi Fei (Northeastern University, USA)</i>	

Track 3 - Session 12: Privacy and ML

SoK: Privacy-Preserving Data Synthesis	4696
<i>Yuzheng Hu (University of Illinois at Urbana Champaign, USA), Fan Wu (University of Illinois at Urbana Champaign, USA), Qinbin Li (UC Berkeley, USA), Yunhui Long (University of Illinois at Urbana Champaign, USA), Gonzalo Garrido (Technische Universität München, Germany), Chang Ge (University of Minnesota, USA), Bolin Ding (Alibaba Group, USA), David Forsyth (University of Illinois at Urbana Champaign, USA), Bo Li (University of Illinois at Urbana Champaign, USA), and Dawn Song (UC Berkeley, USA)</i>	
Preserving Node-level Privacy in Graph Neural Networks	4714
<i>Zihang Xiang (King Abdullah University of Science and Technology, KSA), Tianhao Wang (University of Virginia, USA), and Di Wang (King Abdullah University of Science and Technology)</i>	
From Principle to Practice: Vertical Data Minimization for Machine Learning	4733
<i>Robin Staab (ETH Zurich, Switzerland), Nikola Jovanović (ETH Zurich, Switzerland), Mislav Balunović (ETH Zurich, Switzerland), and Martin Vechev (ETH Zurich, Switzerland)</i>	
BOLT: Privacy-Preserving, Accurate and Efficient Inference for Transformers	4753
<i>Qi Pang (Carnegie Mellon University), Jinhao Zhu (UC Berkeley), Helen Möllering (Technical University of Darmstadt), Wenting Zheng (Carnegie Mellon University), and Thomas Schneider (Technical University of Darmstadt)</i>	
SHERPA: Explainable Robust Algorithms for Privacy-Preserved Federated Learning in Future Networks to Defend Against Data Poisoning Attacks	4772
<i>Chamara Sandeepa (University College Dublin, Ireland), Bartłomiej Siniarski (University College Dublin, Ireland), Shen Wang (University College Dublin, Ireland), and Madhusanka Liyanage (University College Dublin, Ireland)</i>	
Please Tell Me More: Privacy Impact of Explainability through the Lens of Membership Inference Attack	4791
<i>Han Liu (Washington University in St. Louis, USA), Yuhao Wu (Washington University in St. Louis, USA), Zhiyuan Yu (Washington University in St. Louis, USA), and Ning Zhang (Washington University in St. Louis, USA)</i>	
From Individual Computation to Allied Optimization: Remodeling Privacy-Preserving Neural Inference with Function Input Tuning	4810
<i>Qiao Zhang (Chongqing University, China), Tao Xiang (Chongqing University, China), Chunsheng Xin (Old Dominion University, USA), and Hongyi Wu (The University of Arizona, USA)</i>	
Protecting Label Distribution in Cross-Silo Federated Learning	4828
<i>Yangfan Jiang (National University of Singapore), Xinjian Luo (National University of Singapore), Yuncheng Wu (National University of Singapore), Xiaokui Xiao (National University of Singapore), and Beng Chin Ooi (National University of Singapore)</i>	

Author Index