

Proceedings

**2023**

**Network and Distributed  
System Security Symposium**



Proceedings

**2023**

**Network and Distributed  
System Security Symposium**

February 27 – March 3, 2023

San Diego, CA, USA

*Hosted by the*  
**Internet Society**





---

**Internet Society**  
**11710 Plaza America Drive**  
**Suite 400**  
**Reston, VA 20190**

---

Copyright © 2023 by the Internet Society.  
All rights reserved.

This volume is published as a collective work. The Internet Society owns the copyright for this publication and the copyrights to the individual papers are retained by their respective author[s].

Address your correspondence to: NDSS Program Manager, Internet Society, 11710 Plaza America Drive, Suite 400, Reston, VA 20190 USA, tel. +1 703 439 2120, fax +1 703 326 9881, [ndss@elists.isoc.org](mailto:ndss@elists.isoc.org).

*The papers included here comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interest of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors or the Internet Society.*

ISBN Number (Digital Format) : 1-891562-83-5

*Additional copies may be ordered from:*



**Internet Society**  
11710 Plaza America Drive  
Suite 400  
Reston, VA 20190  
tel +1 703 439 2120  
fax +1 703 326 9881  
<http://www.internetsociety.org>

## **Table of Contents**

**Message from the General Chairs**  
**Message from the Program Committee Co-Chairs**  
**Message from the Internet Society**  
**Program Committee**  
**External Reviewers**  
**Organizing Committee**  
**Steering Group**

### **Session 1A: Software Security I**

Assessing the Impact of Interface Vulnerabilities in Compartmentalized Software

*Hugo Lefeuvre (The University of Manchester); Vlad-Andrei Bădoiu (University Politehnica of Bucharest); Yi Chen (Rice University); Felipe Huici (Unikraft.io); Nathan Dautenhahn (Rice University); Pierre Olivier (The University of Manchester)*

Let Me Unwind That For You: Exceptions to Backward-Edge Protection

*Victor Duta (Vrije Universiteit Amsterdam); Fabian Freyer (unaffiliated); Fabio Pagani (University of California, Santa Barbara); Marius Muench and Cristiano Giuffrida (Vrije Universiteit Amsterdam)*

VulHawk: Cross-architecture Vulnerability Detection with Entropy-based Binary Code Search

*Zhenhao Luo, Pengfei Wang, Baosheng Wang, Yong Tang, Wei Xie, Xu Zhou, Danjun Liu, and Kai Lu (College of Computer, National University of Defense Technology)*

Towards Automatic and Precise Heap Layout Manipulation for General-Purpose Programs

*Runhao Li, Bin Zhang, Jiongyi Chen, Wenfeng Lin, Chao Feng, and Chaojing Tang (National University of Defense Technology)*

### **Session 1B: ML and AI I**

Backdoor Attacks Against Dataset Distillation

*Yugeng Liu, Zheng Li, and Michael Backes (CISPA Helmholtz Center for Information Security); Yun Shen (Netapp); Yang Zhang (CISPA Helmholtz Center for Information Security)*

REaaS: Enabling Adversarially Robust Downstream Classifiers via Robust Encoder as a Service

*Wenjie Qu (Huazhong University of Science and Technology); Jinyuan Jia (University of Illinois Urbana-Champaign); Neil Zhenqiang Gong (Duke University)*

Adversarial Robustness for Tabular Data through Cost and Utility Awareness

*Klim Kireev, Bogdan Kulynych, and Carmela Troncoso (EPFL)*

Focusing on Pinocchio's Nose: A Gradients Scrutinizer to Thwart Split-Learning Hijacking Attacks Using Intrinsic Attributes

*Jiayun Fu and Xiaojing Ma (Huazhong University of Science and Technology); Bin B. Zhu (Microsoft Research Asia); Pingyi Hu, Ruixin Zhao, Yaru Jia, Peng Xu, and Hai Jin (Huazhong University of Science and Technology); Dongmei Zhang (Microsoft Research)*

### **Session 1C: Privacy and Anonymity I**

ProbFlow: Using Probabilistic Programming in Anonymous Communication Networks  
*Hussein Darir, Geir Dullerud, and Nikita Borisov (University of Illinois Urbana-Champaign)*

PPA: Preference Profiling Attack Against Federated Learning  
*Chunyi Zhou, Yansong Gao, and Anmin Fu (Nanjing University of Science and Technology); Kai Chen (Chinese Academy of Science); Zhiyang Dai (Nanjing University of Science and Technology); Zhi Zhang and Minhui Xue (CSIRO's Data61); Yuqing Zhang (University of Chinese Academy of Science)*

RAI2: Responsible Identity Audit Governing the Artificial Intelligence  
*Tian Dong, Shaofeng Li, and Guoxing Chen (Shanghai Jiao Tong University); Minhui Xue (CSIRO's Data61); Haojin Zhu and Zhen Liu (Shanghai Jiao Tong University)*

Faster Secure Comparisons with Offline Phase for Efficient Private Set Intersection  
*Florian Kerschbaum (University of Waterloo); Erik-Oliver Blass (Airbus); Rasoul Akhavan Mahdavi (University of Waterloo)*

### **Session 2A: Software Security II**

DiffCSP: Finding Browser Bugs in Content Security Policy Enforcement through Differential Testing  
*Seongil Wi (KAIST); Trung Tin Nguyen (CISPA Helmholtz Center for Information Security, Saarland University); Jihwan Kim (KAIST); Ben Stock (CISPA Helmholtz Center for Information Security); Sooel Son (KAIST)*

Browser Permission Mechanisms Demystified  
*Kazuki Nomoto (Waseda University); Takuya Watanabe, Eitaro Shioji, and Mitsuaki Akiyama (NTT Social Informatics Laboratories); Tatsuya Mori (Waseda University/NICT/RIKEN AIP)*

Drone Security and the Mysterious Case of DJI's DroneID  
*Nico Schiller (Ruhr-Universität Bochum); Merlin Chlosta (CISPA Helmholtz Center for Information Security); Moritz Schloegel (Ruhr-Universität Bochum); Nils Bars and Thorsten Eisenhofer (Ruhr University Bochum); Tobias Scharnowski (Ruhr-Universität Bochum); Felix Domke (Independent); Lea Schönherr and Thorsten Holz (CISPA Helmholtz Center for Information Security)*

## Session 2B: ML and AI II

The "Beatrix" Resurrections: Robust Backdoor Detection via Gram Matrices

*Wanlun Ma (Swinburne University of Technology); Derui Wang (CSIRO's Data61); Ruoxi Sun (The University of Adelaide & CSIRO's Data61); Minhui Xue (CSIRO's Data61); Sheng Wen (Swinburne University of Technology); Yang Xiang (Digital Research & Innovation Capability Platform, Swinburne University of Technology)*

RoVISQ: Reduction of Video Service Quality via Adversarial Attacks on Deep Learning-based Video Compression

*Jung-Woo Chang and Mojan Javaheripi (University of California San Diego); Seira Hidano (KDDI Research, Inc.); Farinaz Koushanfar (University of California San Diego)*

Machine Unlearning of Features and Labels

*Alexander Warnecke and Lukas Pirch (TU Braunschweig); Christian Wressneger (Karlsruhe Institute of Technology (KIT)); Konrad Rieck (TU Braunschweig)*

Fusion: Efficient and Secure Inference Resilient to Malicious Servers

*Caiqin Dong, Jian Weng, Jia-Nan Liu, and Yue Zhang (Jinan University); Yao Tong (Guangzhou Fongwell Data Limited Company); Anjia Yang, Yudan Cheng, and Shun Hu (Jinan University)*

## Session 2C: Privacy and Anonymity II

Trellis: Robust and Scalable Metadata-private Anonymous Broadcast

*Simon Langowski, Sacha Servan-Schreiber, and Srinivas Devadas (Massachusetts Institute of Technology)*

On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies

*Piyush Kumar Sharma (imec-COSIC, KU Leuven); Devashish Gosain (Max Planck Institute for Informatics); Claudia Diaz (Nym Technologies, SA and imec-COSIC, KU Leuven)*

Thwarting Smartphone SMS Attacks at the Radio Interface Layer

*Haohuang Wen (Ohio State University); Phillip Porras and Vinod Yegneswaran (SRI International); Zhiqiang Lin (Ohio State University)*

InfoMasker: Preventing Eavesdropping Using Phoneme-Based Noise

*Peng Huang, Yao Wei, Peng Cheng, Zhongjie Ba, Li Lu, Feng Lin, Fan Zhang, and Kui Ren (Zhejiang University)*

## Session 3A: Fuzzing

FUZZILLI: Fuzzing for JavaScript JIT Compiler Vulnerabilities

*Samuel Groß (Google); Simon Koch (TU Braunschweig); Lukas Bernhard (Ruhr-University Bochum); Thorsten Holz (CISPA Helmholtz Center for Information Security); Martin Johns (TU Braunschweig)*

No Grammar, No Problem: Towards Fuzzing the Linux Kernel without System-Call Descriptions

*Alexander Bulekov (Boston University); Bandan Das and Stefan Hajnoczi (Red Hat); Manuel Egele (Boston University)*

DARWIN: Survival of the Fittest Fuzzing Mutators

*Patrick Jauernig (Technical University of Darmstadt); Domagoj Jakobovic (University of Zagreb, Croatia); Stjepan Picek (Radboud University and TU Delft); Emmanuel Stapf and Ahmad-Reza Sadeghi (Technical University of Darmstadt)*

LOKI: State-Aware Fuzzing Framework for the Implementation of Blockchain Consensus Protocols

*Fuchen Ma, Yuanliang Chen, Meng Ren, Yuanhang Zhou, and Yu Jiang (Tsinghua University); Ting Chen (University of Electronic Science and Technology of China); Huizhong Li (WeBank); Jiaguang Sun (School of Software, Tsinghua University)*

### **Session 3B: ML and AI III**

Securing Federated Sensitive Topic Classification against Poisoning Attacks

*Tianyue Chu and Alvaro Garcia-Recuero (IMDEA Networks Institute); Costas Iordanou (Cyprus University of Technology); Georgios Smaragdakis (TU Delft); Nikolaos Laoutaris (IMDEA Networks Institute)*

OBSan: An Out-Of-Bound Sanitizer to Harden DNN Executables

*Yanzuo Chen, Yuanyuan Yuan, and Shuai Wang (The Hong Kong University of Science and Technology)*

BARS: Local Robustness Certification for Deep Learning based Traffic Analysis Systems

*Kai Wang, Zhiliang Wang, Dongqi Han, Wenqi Chen, Jiahai Yang, Xingang Shi, and Xia Yin (Tsinghua University)*

Anomaly Detection in the Open World: Normality Shift Detection, Explanation, and Adaptation

*Dongqi Han, Zhiliang Wang, Wenqi Chen, Kai Wang, Rui Yu, Su Wang, and Han Zhang (Tsinghua University); Zhihua Wang and Minghui Jin (State Grid Shanghai Municipal Electric Power Company); Jiahai Yang, Xingang Shi, and Xia Yin (Tsinghua University)*

### **Session 4A: Network Protocols**

Ghost Domain Reloaded: Vulnerable Links in Domain Name Delegation and Revocation

*Xiang Li and Baojun Liu (Tsinghua University); Xuesong Bai (University of California, Irvine); Mingming Zhang (Tsinghua University); Qifan Zhang and Zhou Li (University of California, Irvine); Haixin Duan (Tsinghua University); QI-ANXIN*

*Technology Research Institute; Zhongguancun Laboratory); Qi Li (Tsinghua University; Zhongguancun Laboratory)*

QUICforge: Client-side Request Forgery in QUIC

*Yuri Gbur and Florian Tschorsch (Technische Universität Berlin)*

Automata-Based Automated Detection of State Machine Bugs in Protocol Implementations

*Paul Fiterau-Brostean and Bengt Jonsson (Uppsala University, Sweden); Konstantinos Sagonas (Uppsala University, Sweden and National Technical University of Athens, Greece); Fredrik Tåquist (Uppsala University, Sweden)*

I Still Know What You Watched Last Sunday: Privacy of the HbbTV Protocol in the European Smart TV Landscape

*Carlotta Tagliaro (TU Wien); Florian Hahn (University of Twente); Riccardo Sepe (Guess Europe Sagl); Alessio Aceti (Sababa Security SpA); Martina Lindorfer (TU Wien)*

Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels

*Long Pan, Jiahai Yang, Lin He, Zhiliang Wang, Leyao Nie, Guanglei Song, and Yaozhong Liu (Tsinghua University)*

## **Session 4B: Blockchains I**

POSE: Practical Off-chain Smart Contract Execution

*Tommaso Frassetto, Patrick Jauernig, David Koisser, David Kretzler, Benjamin Schlosser, Sebastian Faust, and Ahmad-Reza Sadeghi (Technical University of Darmstadt)*

OptRand: Optimistically Responsive Reconfigurable Distributed Randomness

*Adithya Bhat (Purdue University); Nibesh Shrestha (Rochester Institute of Technology); Aniket Kate (Purdue University); Kartik Nayak (Duke University)*

Partitioning Ethereum without Eclipsing It

*Hwanjo Heo (ETRI); Seungwon Woo (ETRI/KAIST); Taeung Yoon, Min Suk Kang, and Seungwon Shin (KAIST)*

Smarter Contracts: Detecting Vulnerabilities in Smart Contracts with Deep Transfer Learning

*Christoph Sendner (University of Wuerzburg); Huili Chen (University of California San Diego); Hossein Fereidooni (Technische Universität Darmstadt); Lukas Petzi, Jan König, Jasper Stang, and Alexandra Dmitrienko (University of Wuerzburg); Ahmad-Reza Sadeghi (Technical University of Darmstadt); Farinaz Koushanfar (University of California San Diego)*

Real Threshold ECDSA

*Harry W. H. Wong, Jack P. K. Ma, Hoover H. F. Yin, and Sherman S. M. Chow (The Chinese University of Hong Kong)*



## **Session 4C: Mobile Security and Privacy**

Post-GDPR Threat Hunting on Android Phones: Dissecting OS-level Safeguards of User-unresettable Identifiers

*Mark Huasong Meng (National University of Singapore); Qing Zhang, Guangshuai Xia, and Yuwei Zheng (ByteDance); Yanjun Zhang and Guangdong Bai (The University of Queensland); Zhi Liu (ByteDance); Sin G. Teo (Agency for Science, Technology and Research); Jin Song Dong (National University of Singapore)*

MyTEE: Own the Trusted Execution Environment on Embedded Devices

*Seungkyun Han and Jinsoo Jang (Chungnam National University)*

StealthyIMU: Stealing Permission-protected Private Information From Smartphone Voice Assistant Using Zero-Permission Sensors

*Ke Sun, Chunyu Xia, Songlin Xu, and Xinyu Zhang (University of California San Diego)*

AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms

*Hossein Fereidooni (Technical University of Darmstadt); Jan Koenig (University of Wuerzburg); Phillip Rieger and Marco Chilese (Technical University of Darmstadt); Bora Goekbakan (KOBIL, Germany); Moritz Finke and Alexandra Dmitrienko (University of Wuerzburg); Ahmad-Reza Sadeghi (Technical University of Darmstadt)*

Do Not Give a Dog Bread Every Time He Wags His Tail: Stealing Passwords through Content Queries (CONQUER) Attacks

*Chongqing Lei and Zhen Ling (Southeast University); Yue Zhang (Jinan University); Kai Dong, Kaizheng Liu, and Junzhou Luo (Southeast University); Xinwen Fu (University of Massachusetts Lowell)*

## **Session 5A: Trustworthy Computing**

RR: A Fault Model for Efficient TEE Replication

*Baltasar Dinis (Instituto Superior Técnico (IST-ULisboa) / INESC-ID / MPI-SWS); ; Peter Druschel (MPI-SWS); Rodrigo Rodrigues (Instituto Superior Técnico (IST-ULisboa) / INESC-ID)*

Copy-on-Flip: Hardening ECC Memory Against Rowhammer Attacks

*Andrea Di Dio (Vrije Universiteit Amsterdam); Koen Koning (Intel); Herbert Bos and Cristiano Giuffrida (Vrije Universiteit Amsterdam)*

Extrapolating Formal Analysis to Uncover Attacks in Bluetooth Passkey Entry Pairing

*Mohit Kumar Jangid (The Ohio State University); Yue Zhang (Computer Science & Engineering, Ohio State University); Zhiqiang Lin (The Ohio State University)*

Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems

*Hadi Abdullah (Visa Research); Aditya Karlekar, Saurabh Prasad, Muhammad Sajidur Rahman, Logan Blue, Luke A. Bauer, Vincent Bindschaedler, and Patrick Traynor (University of Florida)*

## **Session 5B: Blockchains II**

Cryptographic Oracle-based Conditional Payments

*Varun Madathil (North Carolina State University); Sri Aravinda Krishnan Thyagarajan (NTT Research); Dimitrios Vasilopoulos (IMDEA Software Institute); Lloyd Fournier (None); Giulio Malavolta (Max Planck Institute for Security and Privacy); Pedro Moreno-Sanchez (IMDEA Software Institute)*

BlockScope: Detecting and Investigating Propagated Vulnerabilities in Forked Blockchain Projects

*Xiao Yi, Yuzhou Fang, and Daoyuan Wu (The Chinese University of Hong Kong); Lingxiao Jiang (Singapore Management University)*

Breaking and Fixing Virtual Channels: Domino Attack and Donner

*Lukas Aumayr (TU Wien); Pedro Moreno-Sanchez (IMDEA Software Institute); Aniket Kate (Purdue University / Supra); Matteo Maffei (Christian Doppler Laboratory Blockchain Technologies for the Internet of Things / TU Wien)*

He-HTLC: Revisiting Incentives in HTLC

*Sarisht Wadhwa and Jannis Stoeter (Duke University); Fan Zhang (Duke University, Yale University); Kartik Nayak (Duke University)*

## **Session 5C: Keys and Certification**

Parakeet: Practical Key Transparency for End-to-End Encrypted Messaging

*Harjasleen Malvai (UIUC/IC3); Lefteris Kokoris-Kogias (IST Austria); Alberto Sonnino (Mysten Labs); Esha Ghosh (Microsoft Research); Ercan Oztürk, Kevin Lewi, and Sean Lawlor (Meta)*

The Power of Bamboo: On the Post-Compromise Security for Searchable Symmetric Encryption

*Tianyang Chen and Peng Xu (Huazhong University of Science and Technology); Stjepan Picek (Radboud University); Bo Luo (The University of Kansas); Willy Susilo (University of Wollongong); Hai Jin (Huazhong University of Science and Technology); Kaitai Liang (TU Delft)*

Private Certifier Intersection

*Bishakh Chandra Ghosh (Indian Institute of Technology Kharagpur); Sikhar Patranabis, Dhinakaran Vinayagamurthy, Venkatraman Ramakrishna, and Krishnasuri Narayanam (IBM Research - India); Sandip Chakraborty (Indian Institute of Technology Kharagpur)*

OBI: a multi-path oblivious RAM for forward-and-backward-secure searchable encryption

*Zhiqiang Wu (Changsha University of Science and Technology); Rui Li (Dongguan University of Technology)*

## **Session 6A: Cyber-Physical Systems Security I**

Un-Rocking Drones: Foundations of Acoustic Injection Attacks and Recovery Thereof

*Jinseob Jeong (KAIST, Agency for Defense Development); Dongkwan Kim (Samsung SDS); Joonha Jang, Juhwan Noh, Changhun Song, and Yongdae Kim (KAIST)*

EdgeTDC: On the Security of Time Difference of Arrival Measurements in CAN Bus Systems

*Marc Roeschlin, Giovanni Camurati, and Pascal Brunner (ETH Zurich, Switzerland); Mridula Singh (CISPA Helmholtz Center for Information Security); Srdjan Capkun (ETH Zurich, Switzerland)*

Evasion Attacks and Defenses on Smart Home Physical Event Verification

*Muslum Ozgur Ozmen, Ruoyu Song, Habiba Farrukh, and Z. Berkay Celik (Purdue University)*

SoundLock: A Novel User Authentication Scheme for VR Devices Using Auditory-Pupillary Response

*Huadi Zhu, Mingyan Xiao, Demoria Sherman, and Ming Li (The University of Texas at Arlington)*

## **Session 6B: Web Security I**

Accountable Javascript Code Delivery

*Ilkan Esiyok (CISPA Helmholtz Center for Information Security); Pascal Berrang (University of Birmingham & Nimiq); Katriel Cohn-Gordon (Meta); Robert Künnemann (CISPA Helmholtz Center for Information Security)*

ReScan: A Middleware Framework for Realistic and Robust Black-box Web Application Scanning

*Kostas Drakonakis (FORTH); Sotiris Ioannidis (Technical University of Crete); Jason Polakis (University of Illinois at Chicago)*

Him of Many Faces: Characterizing Billion-scale Adversarial and Benign Browser Fingerprints on Commercial Websites

*Shujiang Wu (Johns Hopkins University); Pengfei Sun and Yao Zhao (F5, Inc.); Yinzhi Cao (Johns Hopkins University)*

A Security Study about Electron Applications and a Programming Methodology to Tame DOM Functionalities

*Zihao Jin (Microsoft Research and Tsinghua University); Shuo Chen and Yang Chen (Microsoft Research); Haixin Duan (Tsinghua University and Quancheng Laboratory); Jianjun Chen (Tsinghua University and Zhongguancun Laboratory); Jianping Wu (Tsinghua University)*

## **Session 6C: Cyber-Crime and Forensics**

An OS-agnostic Approach to Memory Forensics

*Andrea Oliveri (EURECOM); Matteo Dell'Amico (University of Genoa); Davide Balzarotti (EURECOM)*

BEAGLE: Forensics of Deep Learning Backdoor Attack for Better Defense

*Siyuan Cheng, Guanhong Tao, Yingqi Liu, Shengwei An, Xiangzhe Xu, Shiwei Feng, Guangyu Shen, Kaiyuan Zhang, and Qiuling Xu (Purdue University); Shiqing Ma (Rutgers University); Xiangyu Zhang (Purdue University)*

Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams

*Xigao Li, Anurag Yepuri, and Nick Nikiforakis (Stony Brook University)*

Preventing SIM Box Fraud Using Device Model Fingerprinting

*BeomSeok Oh, Junho Ahn, Sangwook Bae, Mincheol Son, Yonghwa Lee, Min Suk Kang, and Yongdae Kim (KAIST)*

## **Session 7A: Cyber-Physical Systems Security II**

Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3

*Xinyi Xie, Kun Jiang, Rui Dai, Jun Lu, and Lihui Wang (Shanghai Fudan Microelectronics Group Co., Ltd.); Qing Li and Jun Yu (State Key Laboratory of ASIC & System, Fudan University)*

MetaWave: Attacking mmWave Sensing with Meta-material-enhanced Tags

*Xingyu Chen and Zhengxiong Li (University of Colorado Denver); Baicheng Chen (University of California San Diego); Yi Zhu (SUNY at Buffalo); Chris Xiaoxuan Lu (University of Edinburgh); Zhengyu Peng (Aptiv); Feng Lin (Zhejiang University); Wen Yao Xu (SUNY Buffalo); Kui Ren (Zhejiang University); Chunming Qiao (SUNY at Buffalo)*

Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels

*Joonha Jang, ManGi Cho, Jaehoon Kim, Dongkwan Kim, and Yongdae Kim (KAIST)*

Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging

*Sebastian Köhler and Richard Baker (University of Oxford); Martin Strohmeier (armasuisse Science + Technology); Ivan Martinovic (University of Oxford)*

## **Session 7B: Web Security II**

CHKPLUG: Checking GDPR Compliance of WordPress Plugins via Cross-language Code Property Graph

*Faysal Hossain Shezan and Zihao Su (University of Virginia); Mingqing Kang (Johns Hopkins University); Nicholas Phair and Patrick William Thomas*

*(University of Virginia); Michelangelo van Dam (in2it); Yinzhi Cao (Johns Hopkins University); Yuan Tian (UCLA)*

SynthDB: Synthesizing Database via Program Analysis for Security Testing of Web Applications

*An Chen (University of Georgia); Jiho Lee (University of Virginia); Basanta Chaulagain (University of Georgia); Yonghwi Kwon (University of Virginia); Kyu Hyung Lee (University of Georgia)*

Hope of Delivery: Extracting User Locations From Mobile Instant Messengers

*Theodor Schnitzler (Research Center Trustworthy Data Science and Security, TU Dortmund, and Ruhr-Universität Bochum); Katharina Kohls (Radboud University); Evangelos Bitsikas (Northeastern University and New York University Abu Dhabi); Christina Pöpper (New York University Abu Dhabi)*

Tactics, Threats & Targets: Modeling Disinformation and its Mitigation

*Shujaat Mirza (New York University); Labeeba Begum (New York University Abu Dhabi); Liang Niu (New York University); Sarah Pardo and Azza Abouzied (New York University Abu Dhabi); Paolo Papotti (EURECOM); Christina Pöpper (New York University Abu Dhabi)*

## **Session 7C: Cyber Attacks**

How to Count Bots in Longitudinal Datasets of IP Addresses

*Leon Böck (Technische Universität Darmstadt); Dave Levin (University of Maryland); Ramakrishna Padmanabhan (CAIDA); Christian Doerr (Hasso Plattner Institute); Max Mühlhäuser (Technical University of Darmstadt)*

Sometimes, You Aren't What You Do: Mimicry Attacks against Provenance Graph Host Intrusion Detection Systems

*Akul Goyal (University of Illinois at Urbana-Champaign); Xueyuan Han (Wake Forest University); Gang Wang and Adam Bates (University of Illinois at Urbana-Champaign)*

BinaryInferno: A Semantic-Driven Approach to Field Inference for Binary Message Formats

*Jared Chandler (Tufts University); Adam Wick (Fastly); Kathleen Fisher (DARPA)*

Detecting Unknown Encrypted Malicious Traffic in Real Time via Flow Interaction Graph Analysis

*Chuanpu Fu, Qi Li, and Ke Xu (Tsinghua University)*

## **Session 8A: Cloud and Edge Computing**

Efficient Dynamic Proof of Retrievability for Cold Storage

*Tung Le (Virginia Tech); Pengzhi Huang (Cornell University); Attila A. Yavuz (University of South Florida); Elaine Shi (CMU); Thang Hoang (Virginia Tech)*

HeteroScore: Evaluating and Mitigating Cloud Security Threats Brought by Heterogeneity

*Chongzhou Fang and Najmeh Nazari (University of California, Davis); Behnam Omidi (George Mason University); Han Wang (Temple University); Aditya Puri*

*(Foothill High School, Pleasanton, CA); Manish Arora (LearnDesk, Inc.); Setareh Rafatirad and Houman Homayoun (University of California, Davis); Khaled N. Khasawneh (George Mason University)*

A Robust Counting Sketch for Data Plane Intrusion Detection

*Sian Kim and Changhun Jung (Ewha Womans University); RhongHo Jang (Wayne State University); David Mohaisen (University of Central Florida); DaeHun Nyang (Ewha Womans University)*

REDsec: Running Encrypted Discretized Neural Networks in Seconds

*Lars Wolfgang Folkerts, Charles Gouert, and Nektarios Georgios Tsoutsos (University of Delaware)*

### **Session 8B: Web Security III**

DOITRUST: Dissecting On-chain Compromised Internet Domains via Graph Learning

*Shuo Wang, Mahathir Almashor, and Alsharif Abuadbbba (CSIRO's Data61 & Cybersecurity CRC, Australia); Ruoxi Sun, Minhui Xue, and Calvin Wang (CSIRO's Data61); Raj Gaire, Surya Nepal, and Seyit Camtepe (CSIRO's Data61 & Cybersecurity CRC, Australia)*

VICEROY: GDPR-/CCPA-compliant Enforcement of Verifiable Accountless Consumer Requests

*Scott Jordan, Yoshimichi Nakatsuka, and Ercan Ozturk (University of California, Irvine); Andrew Pavverd (Microsoft Research); Gene Tsudik (University of California, Irvine)*

Navigating Murky Waters: Automated Browser Feature Testing for Uncovering Tracking Vectors

*Mir Masood Ali (University of Illinois Chicago); Binoy Chitale (Stony Brook University); Mohammad Ghasemisharif and Chris Kanich (University of Illinois Chicago); Nick Nikiforakis (Stony Brook University); Jason Polakis (University of Illinois Chicago)*

ChargePrint: A Framework for Internet-Scale Discovery and Security Analysis of EV Charging Management Systems

*Tony Nasr (Concordia University); Sadegh Torabi (George Mason University); Elias Bou-Harb (University of Texas at San Antonio); Claude Fachkha (University of Dubai); Chadi Assi (Concordia University)*

### **Session 8C: Usable Security and Privacy**

A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites

*Sanam Ghorbani Lyastani (CISPA Helmholtz Center for Information Security, Saarland University); Michael Backes and Sven Bugiel (CISPA Helmholtz Center for Information Security)*

Privacy-Preserving Database Fingerprinting

*Tianxi Ji (Texas Tech University); Erman Ayday (Case Western Reserve University); Emre Yilmaz (University of Houston-Downtown); Ming Li (CSE*

*Department, The University of Texas at Arlington); Pan Li (Case Western Reserve University)*

Folk Models of Misinformation on Social Media

*Filipo Sharevski, Amy Devine, Emma Pieroni, and Peter Jachim (DePaul University)*

Fine-Grained Trackability in Protocol Executions

*Ksenia Budykho, Ioana Boureanu, and Steve Wesemeyer (Surrey Centre for Cyber Security, University of Surrey, UK); Daniel Romero and Matt Lewis (NCC Group); Yogaratnam Rahulan (5G/6G Innovation Centre - 5GIC/6GIC, University of Surrey, UK); Fortunat Rajaona and Steve Schneider (Surrey Centre for Cyber Security, University of Surrey, UK)*

## Message from the General Chairs

Welcome to the 2023 Network and Distributed System Security (NDSS) Symposium! We're excited that this is our 30-year anniversary, and that you are here to celebrate with us!

Fun fact: if you go to the NDSS website, you will see that the first proceedings posted are from 1993. The astute among us will realize that this means that 2023 should be the 31st year, but it's not so! In 1993, NDSS was actually a workshop that was co-hosted by the Internet Society (ISOC) and Lawrence Livermore National Laboratory. The workshop was so successful, that ISOC agreed to host it the following year, as a symposium instead of a workshop, and they have been hosting it ever since!

NDSS has grown in the past 30 years! In 1994, there were 15 papers, three panels and one guest speaker. This year, there are 94 papers and two keynote speakers, along with six co-hosted workshops and two co-located symposia, a special session at NDSS that will give the highlights from each of the co-located events, birds-of-a-feather sessions, a poster session, and a special session celebrating 30 years.

Of course, a program like this could not be put together without the tireless efforts from a large number of volunteers, and they all deserve a huge amount of thanks. First, we'd like to thank our Program Committee Co-Chairs, Wenyuan Xu and Mathias Payer, who have put together a fantastic program, including organizing our first ever workshop highlights session so that the NDSS community who were unable to attend the co-located events can still benefit from learning what was discussed at them.

Similar to previous years, NDSS 2023 had two submission phases, and thanks goes to the co-chairs, the 112 program committee members, and the external reviewers for their work in reviewing paper submissions, shepherding them through major and minor revisions, and selecting the best papers to be presented. A special thanks also goes to David Balenson as publications chair for collecting the camera-ready papers and ensuring they are published.

We would like to also thank Ben Stock and Xiajing Liao for selecting a dynamic set of associated workshops and symposia. This year we are excited to host:

- 1) Symposium on Vehicle Security and Privacy (VehicleSec);
- 2) Workshop on Binary Analysis Research (BAR);
- 3) Learning from Authoritative Security Experiment Results (LASER) Workshop;
- 4) Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb);
- 5) Workshop on Ethics in Computer Security (Ethics);
- 6) Workshop on Security of Space and Satellite Systems (SpaceSec);
- 7) Workshop on Security Operation Center Operations and Construction (WOSOC); and
- 8) Usable Security and Privacy (USEC) Symposium.



Three of the workshops continue from last year along with one symposium. There are three entirely new workshops this year, and we're thrilled to welcome VehicleSec back to NDSS as a symposium rather than a workshop (previously named AutoSec). We would also like to thank VehicleSec for co-sponsoring the NDSS Welcome Reception.

There are many other people who have helped make NDSS 2023 a success, and we would like to thank Alexandra Dmitrienko and Tiffany Bao for putting together a wonderful poster session this year, including organizing the best poster awards. We would also like to thank Pedro Moreno-Sanchez and his team for reviewing the student grant applications resulting in support for 18 students, Brendan Saltaformaggio and Ramjita Pai Kasturi for publicity, and Tom Hutton as local arrangements chair. And the Steering Committee deserves thanks for their active participation and wise advice.

We also want to provide a special thank you to Ahmad-Reza Sadeghi and Ben Stock for putting together the 30-year anniversary celebration session, including the fun video that gives us a blast from the past! Another special thank you to Mathias Payer for providing an overview of the previous test-of-time winners to highlight the impact that NDSS has had on the security community. And thanks to CISPAs for supporting the Wednesday night anniversary celebration!

NDSS is possible in large part thanks to our generous sponsors, and we'd like to thank (in alphabetical order) sponsorship from the following companies (including organizations that sponsored VehicleSec): ASU Global Security Initiative, BlockSec, Check Point, Cybertruck Challenge, ETAS, Futurewei Technologies, GM, Google, Huawei, IBM, Meta, National Science Foundation, Netflix, Palo Alto Networks, Qualcomm, TikTok, and Zoox.

NDSS would not happen if it were not for the incredible support from Karen O'Donoghue and her team – thank you!! And thank you to the Internet Society for their continued support of NDSS for the past 30 years, and to the Association Management Solutions (AMS) staff.

Finally, thank you to all of you!! Your participation in NDSS is the reason we exist, and we would love to thank you for 30 years of support building a warm community around this symposium. We hope that you enjoy NDSS 2023 and our anniversary celebrations!

**Carrie Gates and Cristina Nita-Rotaru  
General Chairs, NDSS 2023**

## Message from the Program Committee Co-Chairs

It is our great pleasure to present to you the technical program of the 2023 Network and Distributed System Security (NDSS) symposium, held as a hybrid event between February 28 and March 3, 2023. For the past 30 years, NDSS has established itself as one of the top conferences in systems security and network security. Papers published at NDSS have made a significant impact on research and practice, as exemplified by the awardees of the NDSS Test-of-Time Award. Our goal continues to be “impact”, especially in the form of novel and practical solutions and techniques in cybersecurity. We hope that the papers in this year’s program reflect the same strong potential in securing real-world networks and systems.

This year we received a total of 574 complete submissions (i.e., not counting papers that clearly violated the submission guidelines). Submissions were evaluated on the basis of their technical quality, novelty, and significance. Multiple rounds of reviewing culminated in two online discussion periods. At the end of the review process, 94 papers (16.4% acceptance rate) were selected to appear in the program. We strove to make the review process a competitive but constructive one. Program Committee (PC) members were regularly reminded to identify positive points in the submission and provide concrete suggestions to improve each paper. Each paper received two initial reviews and, if either review identified positive feedback it advanced to the second round for another set of reviews. Later for each author rebuttal, which was solicited after all reviews were in, we required the corresponding reviews be updated to respond to the rebuttal, to help improve the quality, timeliness, and responsiveness of the review process.

Organizing a conference as large as NDSS is a substantial endeavor, and we would like to extend our sincere thanks to everyone who contributed their time and effort. We would like to specifically thank a few individuals who made particular contributions to NDSS 2023. General Chair Carrie Gates and Cristina Nita-Rotaru oversaw the conference and worked closely with us for Keynote Speaker. Karen O'Donoghue served as a critical interface between the Program Co-Chairs, the Organizing Committee, and ISOC. Publicity Co-Chairs Brendan Saltaformaggio and Ranjita Pai Kasturi worked seamlessly with us to solicit submissions and promote the conference. Publications Chair David Balenson took excellent care of the proceedings production matters. Our special thanks also go to Chen Yan from Zhejiang University for their continuous effort in maintaining the submission system, supporting the PC Co-Chairs during the reviewing process, and planning the event schedule.

Last but not least, we would like to thank our PC members and the external reviewers. The PC members have contributed significant time and effort to the creation of the technical program. It has been our privilege working with them. Finally, we thank all authors who submitted to NDSS 2023 and all attendees who are virtually joining us at NDSS 2023, without whom NDSS would not be possible. Enjoy the conference!

**Wenyuan Xu and Mathias Payer**  
**Program Committee Co-Chairs, NDSS 2023**

## Message from the Internet Society

The Internet Society is proud to host the 30th edition of the Network and Distributed System Security (NDSS) Symposium, one of the world's premier conferences for computer and network security research. Our involvement with NDSS spans this entire period and is a testament to the recognition and support this event receives from the research community both in academia and industry.

A key focus of the Internet Society is improving the security and trustworthiness of the global open Internet. NDSS 2023 brings together leading academics, industry researchers, students, and security practitioners to discuss high-quality peer-reviewed research and to exchange ideas. There is also a strong focus on student participation with the aim of fostering the next generation of leaders in security and privacy.

The Internet Society is committed to using the Internet to improve access to research and to exchange ideas. NDSS 2023 is the second year that we're supporting a hybrid event which is being held over five full days and includes a record eight co-located events including two symposia (VehicleSec and USEC), and six workshops (WOSOC, EthICS, SpaceSec, MADWeb, LASER and BAR), 94 paper presentations, two keynotes, and 34 posters. We're also very pleased to welcome keynote speakers Richard Ford (Praetorian) who is discussing ChatGPT and what this means for machine learning for cybersecurity and privacy, and Nina Taft (Google) who is discussing the challenges developers face with respect to continually evolving privacy laws, policies, and user preferences.

Of course, NDSS 2023 relies very heavily on volunteers from the community to help put together this high-quality program. We are grateful for the hard work undertaken by General Co-Chairs Carrie Gates and Cristina Nita-Rotaru, Program Committee Co-Chairs Wenyuan Xu and Mathias Payer, along with the other members of the Organizing and Program Committees who have invested countless hours to review papers and posters, organize the co-located events, publicize the event, and publish the papers.

Finally, we must thank the sponsors without whom this event would not be possible. This includes our Gold Sponsors Google, the National Science Foundation and TikTok; our T-shirt sponsor BlockSec; our Silver Sponsors Check Point, Futurewei Technologies, Huawei, IBM, Meta, Netflix and Palo Alto Networks; our Lanyard Sponsor Qualcomm; our Reception Sponsor ASU Global Security Initiative; and our VehicleSec Symposium Sponsors ASU Global Security Initiative, Cybertruck Challenge, ETAS, General Motors, the National Science Foundation, Qualcomm and Zoox. We continue to be grateful for the support provided by San Diego Supercomputing Center and USENIX.

On behalf of the Internet Society, I welcome you to NDSS 2023 and hope you have an enjoyable and productive week.

**Andrew Sullivan**  
**CEO, Internet Society**

# Program Committee

Wenyaun Xu, *Zhejiang University (Co-Chair)*

Mathias Payer, *EPFL (Co-Chair)*

Ahmad-Reza Sadeghi, *Technical University of Darmstadt*

Alessandro Sorniotti, *IBM Research*

Alexandra Dmitrienko, *University of Wuerzburg*

Alvaro Cardenas, *UC Santa Cruz*

Anh Dinh, *Singapore University of Technology and Design*

Anil Kurmus, *IBM Research Europe – Zurich*

Antonio Bianchi, *Purdue University*

Ardalan Amiri Sani, *UC Irvine*

Arthur Gervais, *Imperial College London*

Benjamin Andow, *Google*

Benjamin Beurdouche, *Mozilla*

Brendan Saltaformaggio, *Georgia Institute of Technology*

Brent ByungHoon Kang, *KAIST*

Chao Shen, *Xi'an Jiaotong University*

Christina Garman, *Purdue University*

Christina Pöpper, *New York University Abu Dhabi*

Christopher Liebchen, *Google*

Daniel Holcomb, *UMass Amherst*

Daniele Antonioli, *EURECOM*

Daniele Cono D'Elia, *Sapienza University of Rome*

Ding Wang, *Nankai University*

Doowon Kim, *University of Tennessee, Knoxville*

Emiliano De Cristofaro, *UCL*

Fengwei Zhang, *Southern University of Science and Technology (SUSTech)*

Flavio Toffalini, *EPFL*

Frederik Braun, *Mozilla*

Gang Qu, *University of Maryland*

Gang Wang, *University of Illinois at Urbana-Champaign*

Gianluca Stringhini, *Boston University*

Guofei Gu, *Texas A&M*

Haibin Zhang, *Beijing Institute of Technology*

Haipeng Cai, *Washington State University*

Hamed Okhravi, *MIT Lincoln Laboratory*

Haojin Zhu, *Shanghai Jiao Tong University*

Hong Hu, *Penn State University*

Houman Homayoun, *UC Davis*

Ivan De Oliveira Nunes, *Rochester Institute of Technology*

Jason (Minhui) Xue, *CSIRO's Data61*

Jeyavijayan Rajendran, *Texas A&M University*  
Joel Frank, *Ruhr-Universität Bochum*  
Johanna Sepulveda, *Airbus Defence and Space*  
Jon McCune, *Google*  
Jun Xu, *The University of Utah*  
Kangjie Lu, *University of Minnesota*  
Kapil Singh, *IBM T.J. Watson Research Center*  
Karl Wüst, *CISPA Helmholtz Center for Information Security*  
Katharina Krombholz, *CISPA Helmholtz Center for Information Security*  
Kelsey Fulton, *University of Maryland*  
Kun Sun, *George Mason University*  
Lannan Luo, *University of South Carolina*  
Lejla Batina, *Radboud University*  
Limin Jia, *CMU*  
Lucas Davi, *University of Duisburg-Essen*  
Manuel Egele, *Boston University*  
Marcel Busch, *EPFL*  
Marcus Peinado, *Microsoft Research*  
Markus Miettinen, *Technical University of Darmstadt*  
Mauro Conti, *University of Padua*  
Michael Schwarz, *CISPA Helmholtz Center for Information Security*  
Mihalis Maniatakos, *New York University Abu Dhabi*  
Mu Zhang, *University of Utah*  
Nathan Malkin, *University of Maryland*  
Neil Gong, *Duke University*  
Nele Mentens, *Leiden University and KU Leuven*  
Norrathep Rattanavipanon, *Prince of Songkla University, Phuket Campus*  
Pedro Moreno-Sanchez, *IMDEA Software Institute*  
Qi Alfred Chen, *UC Irvine*  
Qi Li, *Tsinghua University*  
Qiang Tang, *The University of Sydney*  
Ren Zhang, *Nervos*  
Saman Zonouz, *Rutgers University*  
Samuel Jero, *MIT Lincoln Laboratory*  
Santiago Torres-Arias, *Purdue University*  
Sarah Zennou, *Airbus*  
Sazzadur Rahaman, *University of Arizona*  
Selcuk Uluagac, *Florida International University*  
Srdjan Capkun, *ETH Zurich*  
Srdjan Matic, *IMDEA Software Institute*  
Stefan Brunthaler, *μCSRL, CODE, UniBwM*  
Stefanie Roos, *TU Delft*  
Stjepan Picek, *TU Delft, The Netherlands*

Syed Rafiul Hussain, *Pennsylvania State University*  
Taegyu Kim, *Pennsylvania State University*  
Tianhao Wang, *University of Virginia*  
Tiffany Bao, *Arizona State University*  
Ting Chen, *University of Electronic Science and Technology of China*  
Trent Jaeger, *Penn State University*  
William Robertson, *Northeastern University*  
Xiaoyu Ji, *Zhejiang University*  
Xiapu Luo, *The Hong Kong Polytechnic University*  
Xinyang Ge, *Netflix*  
Yan Shoshitaishvili, *Arizona State University*  
Yang Zhang, *CISPA Helmholtz Center for Information Security*  
Yanick Fratantonio, *Google*  
Yanjiao Chen, *Zhejiang University*  
Yongdae Kim, *KAIST*  
Yuan Tian, *University of Virginia*  
Yuseok Jeon, *Ulsan National Institute of Science and Technology (UNIST)*  
Z. Berkay Celik, *Purdue University*  
Zahra Ghodsi, *UC San Diego*  
Zhenkai Liang, *National University of Singapore*  
Zhou Li, *University of California, Irvine*

## External Reviewers

Adam Caulfield, *Rochester Institute of Technology*  
Ala' Darabseh, *New York University Abu Dhabi*  
Alexander Bulekov, *Boston University*  
Andrea Mambretti, *IBM Research Europe - Zurich*  
Antonio Joia Neto, *Rochester Institute of Technology*  
Ashwin Nambiar, *Purdue University*  
BeomSeok Oh, *KAIST*  
Cheoljun Park, *KAIST*  
Christian Niesler, *University of Duisburg-Essen*  
Constantine Dومانidis, *New York University Abu Dhabi*  
Darion Cassel, *Carnegie Mellon University*  
David Paaßen, *University of Duisburg-Essen*  
Dohyun Kim, *KAIST*  
Dongkwan Kim, *KAIST*  
Eduardo Chielle, *New York University Abu Dhabi*  
Erin Kenney, *New Jersey Institute of Technology*  
Habiba Farrukh, *Purdue University*  
Hanwen Feng, *University of Sydney*  
Haoran Yang, *Washington State University*  
Hocheol Shin, *Hyundai Motors*  
Homer Gamil, *New York University*  
Huancheng Zhou, *Texas A&M University*  
Hyoungshick Kim, *Sungkyunkwan University*  
Hyungsub Kim, *Purdue University*  
Insu Yun, *KAIST*  
Jaehoon Kim, *KAIST*  
Jens-Rene Giesen, *University of Duisburg-Essen*  
Jiacen Xu, *UC Irvine*  
Jiahao Cao, *Tsinghua University*  
Jianwei Huang, *Texas A&M University*  
Jiho Lee, *KAIST*  
Jiyue Huang, *TU Delft*  
Joann Qiongna Chen, *UC Irvine*  
Joonha Jang, *KAIST*  
Junho Ahn, *KAIST*  
Kexin Hu, *Chinese Academy of Sciences*  
Labeeba Begum, *New York University Abu Dhabi*  
Liam Tyler, *Rochester Institute of Technology*  
Liang Niu, *New York University Abu Dhabi*  
Manaar Alam, *New York University Abu Dhabi*  
Mangi Cho, *KAIST*  
Mi Song, *Nankai University*

Mincheol Son, *KAIST*  
 Muslum Ozgur Ozmen, *Purdue University*  
 Nian Xue, *New York University Abu Dhabi*  
 Oguzhan Ersoy, *Radboud University*  
 Oleg Mazonka, *New York University Abu Dhabi*  
 Omid Aramoon, *University of Maryland*  
 Oussama Draissi, *University of Duisburg-Essen*  
 Pengfei Qiu, *Beijing University of Posts and Telecommunications*  
 Phakpoom Chinprutthiwong, *Sisaket Rajabhat University*  
 Prashant Hari Narayan Rajput, *New York University*  
 Qifan Zhang, *UC Irvine*  
 Qingxuan Wang, *Nankai University*  
 Rujia Li, *Tsinghua University*  
 Ruoyu Wu, *Purdue University*  
 Sangwook Bae, *KAIST*  
 Satwik Prabhu Kumble, *TU Delft*  
 Sebastian Surminski, *University of Duisburg-Essen*  
 Shinjo Park, *TU Berlin*  
 Shreyas Kumar, *Texas A&M University*  
 Shu Wang, *George Mason University*  
 Shuaiqi Wang, *Carnegie Mellon University*  
 Shujaat Mirza, *New York University Abu Dhabi*  
 Sisi Duan, *Tsinghua University*  
 Sung Min (Kevin) Hong, *Texas A&M University*  
 Tian Qiu, *University of Sydney*  
 Tobias Cloosters, *University of Duisburg-Essen*  
 Vicram Rajagopalan, *Texas A&M University*  
 Wen Li, *Washington State University*  
 Xinda Wang, *George Mason University*  
 Xinrui Zhang, *University of Sydney*  
 Xu He, *George Mason University*  
 Xuewei Feng, *Tsinghua University*  
 Yanan Li, *University of Sydney*  
 Yu Nong, *Washington State University*  
 Yu Yu, *Shanghai Jiaotong University*  
 Yuan Lu, *Chinese Academy of Sciences*  
 Yue Wang, *New York University*  
 Yuncong Zhang, *Shanghai Jiaotong University*  
 Yunkai Zou, *Nankai University*  
 Yunwen Liu, *Cryptape Co. Ltd.*  
 Zeyu Lei, *Purdue University*  
 Zhaojun Lu, *Huzhong University of Science and Technology*  
 Zhenliang Lu, *University of Sydney*  
 Zhijie Ren, *Shanghai Shanda Networking Development Co. Ltd.*



# Organizing Committee

## General Chairs

**Carrie Gates**  
*Bank of America*

**Cristina Nita-Rotaru**  
*Northeastern University*

## Program Committee Co-Chairs

**Wenyuan Xu**  
*Zhejiang University*

**Mathias Payer**  
*EPFL*

## Workshop Co-Chairs

**Ben Stock**  
*CISPA Helmholtz Center for  
Information Security*

**Xiaojing Liao**  
*Indiana University*

## Poster Session Co-Chairs

**Alexandra Dmitrienko**  
*University of Würzburg*

**Tiffany Bao**  
*Arizona State University*

## Publicity Co-Chairs

**Brendan Saltaformaggio**  
*Georgia Tech*

**Mingxuan Yao**  
*Georgia Tech*

## Historian and Publications Chair

**David Balenson**  
*USC Information Sciences Institute*

## Past General Chair

**Trent Jaeger**  
*Pennsylvania State University*

## Local Arrangements Chair

**Thomas Hutton**  
*San Diego Supercomputer Center*

## Event Manager

**Karen O'Donoghue**  
*Internet Society*

## Student Support Committee

**Pedro Moreno-Sanchez (Chair)**  
*IMDEA Software Institute*

**Lukas Aumayr**  
*TU Wien*

**Georgia Avarikioti**  
*TU Wien*

**Diego Castejon-Molina**  
*IMDEA Software Institute*

**Debajyoti Das**  
*KU Leuven*

**Yanjiao Chen**  
*Zhejiang University*

**Oguzhan Ersoy**  
*Radboud University*

**Andreas Erwig**  
*TU Darmstadt*

**Noemi Glaeser**  
*University of Maryland*

**Duc Le**  
*University of Bern*

**Varun Madathil**  
*North Carolina State University*

**Easwar Mangipudi**  
*Supra Labs*

**Chrysoula Oikonomou**  
*IMDEA Software Institute*

**Sazzadur Rahaman**  
*University of Arizona*

**Stefanie Roos**  
*TU Delft*

**Clara Schneidewind**  
*MPI-SP*

**Erkan Tairi**  
*TU Wien*

# Steering Group

## Co-Chairs

**Carrie Gates**  
*Bank of America*

**Karen O'Donoghue**  
*Internet Society*

## Steering Group Members

**David Balenson**  
*USC Information Sciences Institute*

**Cristina Nita-Rotaru**  
*Northeastern University*

**Gabriela Ciocarlie**  
*University of Texas San Antonio*

**Mathias Payer**  
*EPFL*

**Tom Hutton**  
*San Diego Supercomputer Center*

**Ahmad-Reza Sadeghi**  
*Technische Universität Darmstadt*

**Trent Jaeger**  
*Pennsylvania State University*

**Deborah Shands**  
*SRI International*

**Chris Kruegel**  
*University of California, Santa Barbara*

**Dongyan Xu**  
*Purdue University*

**Zhenkai Liang**  
*National University of Singapore*

**Wenyuan Xu**  
*Zhejiang University*

**Sarah Meiklejohn**  
*University College London*

**Daphne Yao**  
*Virginia Tech University*

**Anita Nikolich**  
*University of Illinois*