Proceedings

2024

Network and Distributed System Security Symposium

NDSS

SYMPOSIUM

Proceedings

2024

Network and Distributed System Security Symposium

February 26 – March 1, 2024

San Diego, CA, USA

Hosted by the

Internet Society

Internet Society

.

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

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.

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) : 1-891562-93-2

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: Firmware

Decentralized Information-Flow Control for ROS2
Nishit V. Pandya, Himanshu Kumar, Gokulnath M. Pillai, Vinod Ganapathy (Indian Institute of Science Bangalore)

Facilitating Non-Intrusive In-Vivo Firmware Testing with Stateless Instrumentation
Jiameng Shi (University of Georgia); Wenqiang Li (Independent Researcher); Wenwen Wang, Le Guan (University of Georgia)

LDR: Secure and Efficient Linux Driver Runtime for Embedded TEE Systems
Huaiyu Yan, Zhen Ling, Haobo Li (Southeast University); Lan Luo (Anhui University of Technology); Xinhui Shao, Kai Dong, Ping Jiang, Ming Yang (Southeast University); Junzhou Luo (Southeast University, Nanjing, P.R. China); Xinwen Fu (University of Massachusetts Lowell)

Session 1B: Censorship

Content Censorship in the InterPlanetary File System
Srivatsan Sridhar (Stanford University); Onur Ascigil (Lancaster University); Navin Keizer (University College London); François Genon, Sébastien Pierre (UCLouvain); Yiannis Psaras (Protocol Labs); Etienne Rivière (UCLouvain); Michał Król (City, University of London)
Censorship

On Precisely Detecting Censorship Circumvention in Real-World Networks
Ryan Wails (Georgetown University, U.S. Naval Research Laboratory); George Arnold Sullivan (University of California, San Diego); Micah Sherr (Georgetown University); Rob Jansen (U.S. Naval Research Laboratory)

Modeling and Detecting Internet Censorship Events
Elisa Tsai, Ram Sundara Raman, Atul Prakash, Roya Ensafi (University of Michigan)

Session 1C: Applied Cryptography

Efficient and Timely Revocation of V2X Credentials
Gianluca Scopelliti (Ericsson & KU Leuven); Christoph Baumann (Ericsson); Fritz Alder, Eddy Truyen (KU Leuven); Jan Tobias Mühlberg (Université libre de Bruxelles & KU Leuven)

Towards Precise Reporting of Cryptographic Misuses
Yikang Chen (The Chinese University of Hong Kong), Yibo Liu (Arizona State University), Ka Lok Wu (The Chinese University of Hong Kong); Duc V Le (Visa Research); Sze Yiu Chau (The Chinese University of Hong Kong)

Unified Symbolic Analysis of WireGuard
Sylvain Ruhault (Agence Nationale de la Sécurité des Systemes d'Information); Pascal Lafourcade, Dhekra Mahmoud (Universite Clermont Auvergne)

Session 2A: Fuzz-all-the-things!

ReqsMiner: Automated Discovery of CDN Forwarding Request Inconsistencies and DoS Attacks with Grammar-based Fuzzing
Linkai Zheng, Xiang Li, Chuhan Wang, Run Guo (Tsinghua University); Haixin Duan (Tsinghua University; Quancheng Laboratory); Jianjun Chen, Chao Zhang (Tsinghua University; Zhongguancun Laboratory); Kaiwen Shen (Tsinghua University)

Large Language Model guided Protocol Fuzzing
Ruijie Meng (National University of Singapore, Singapore); Martin Mirchev (National University of Singapore); Marcel Böhme (MPI-SP, Germany and Monash University, Australia); Abhik Roychoudhury (National University of Singapore)

ShapFuzz: Efficient Fuzzing via Shapley-Guided Byte Selection
Kunpeng Zhang (Shenzhen International Graduate School, Tsinghua University); Xiaogang Zhu (Swinburne University of Technology); Xi Xiao (Shenzhen International Graduate School, Tsinghua University); Minhui Xue (CSIRO's Data61); Chao Zhang (Tsinghua University); Sheng Wen (Swinburne University of Technology)

Session 2B: Tor and Mixed Networks

Flow Correlation Attacks on Tor Onion Service Sessions with Sliding Subset Sum
Daniela Lopes (INESC-ID / IST, Universidade de Lisboa); Jin-Dong Dong (Carnegie Mellon University); Daniel Castro (INESC-ID / IST, Universidade de Lisboa); Pedro Medeiros (INESC-ID / IST, Universidade de Lisboa); Diogo Barradas (University of Waterloo); Bernardo Portela (INESC-ID / IST, Universidade de Lisboa); João Vinagre (INESC TEC / Universidade do Porto); Bernardo Ferreira (LASIGE, Faculdade de Ciências, Universidade de Lisboa); Nicolas Christin (Carnegie Mellon University); Nuno Santos (INESC-ID / IST, Universidade de Lisboa)

MirageFlow: A New Bandwidth Inflation Attack on Tor
Christoph Sendner, Jasper Stang, Alexandra Dmitrienko (University of Würzburg); Raveen Wijewickrama, Murtuza Jadliwala (University of Texas at San Antonio)

LARMix: Latency-Aware Routing in Mix Networks
Mahdi Rahimi, Piyush Kumar Sharma, Claudia Diaz (KU Leuven)

Session 2C: Resource PKI

The CURE to Vulnerabilities in RPKI Validation
Donika Mirdita (Technische Universität Darmstadt); Haya Schulmann, Niklas Vogel (Goethe-Universität Frankfurt); Michael Waidner (Technische Universität Darmstadt, Fraunhofer SIT)

dRR: A Decentralized, Scalable, and Auditable Architecture for RPKI Repository
Yingying Su, Dan Li (Tsinghua university); Li Chen (Zhongguancun Laboratory); Qi Li (Tsinghua university); Sitong Ling (Tsinghua University)

IRRedicator: Pruning IRR with RPKI-Valid BGP Insights
Minhyeok Kang (Seoul National University); Weitong Li (Virginia Tech); Roland van Rijswijk-Deij (University of Twente); Ted "Taekyoung" Kwon (Seoul National University); Taejoong Chung (Virginia Tech)

Session 3A: Routing

Proof of Backhaul: Trustfree Measurement of Broadband Bandwidth
Peiyao Sheng (Kaleidoscope Blockchain Inc.); Nikita Yadav (Indian Institute of Science); Vishal Sevani, Arun Babu, Anand Svr (Kaleidoscope Blockchain Inc.); Himanshu Tyagi (Indian Institute of Science); Pramod Viswanath (Kaleidoscope Blockchain Inc.)

Understanding the Implementation and Security Implications of Protective DNS Services
Mingxuan Liu (Zhongguancun Laboratory; Tsinghua University); Yiming Zhang, Xiang Li, Chaoyi Lu, Baojun Liu (Tsinghua University); Haixin Duan (Tsinghua University; Zhongguancun Laboratory); Xiaofeng Zheng (Institute for Network Sciences and Cyberspace, Tsinghua University; QiAnXin Technology Research Institute & Legendsec Information Technology (Beijing) Inc.)

BGP-iSec: Improved Security of Internet Routing Against Post-ROV Attacks
Cameron Morris, Amir Herzberg, Bing Wang, Samuel Secondo (University of Connecticut)

Symphony: Path Validation at Scale
Anxiao He, Jiandong Fu, Kai Bu, Ruiqi Zhou, Chenlu Miao, Kui Ren (Zhejiang University)

Session 3B: Android and Deserialization

Beyond the Surface: Uncovering the Unprotected Components of Android Against Overlay Attack
Hao Zhou (The Hong Kong Polytechnic University); Shuohan Wu (The Hong Kong Polytechnic University); Chenxiong Qian (University of Hong Kong); Xiapu Luo (The Hong Kong Polytechnic University); Haipeng Cai (Washington State University); Chao Zhang (Tsinghua University)

50 Shades of Support: A Device-Centric Analysis of Android Security Update
Abbas Acar (Florida International University); Güliz Seray Tuncay (Google); Esteban Luques, Harun Oz, Ahmet Aris, Selcuk Uluagac (Florida International University)

QUACK: Hindering Deserialization Attacks via Static Duck Typing
Yaniv David (Columbia University); Neophytos Christou (Brown University); Andreas D. Kellas (Columbia University); Vasileios P. Kemerlis (Brown University); Junfeng Yang (Columbia University)

Automatic Policy Synthesis and Enforcement for Protecting Untrusted Deserialization
Quan Zhang, Yiwen Xu, Zijing Yin, Chijin Zhou, Yu Jiang (Tsinghua University)

Session 3C: Federated Learning

FP-Fed: Privacy-Preserving Federated Detection of Browser Fingerprinting
Meenatchi Sundaram Muthu Selva Annamalai (University College London); Igor Bilogrevic (Google); Emiliano De Cristofaro (University of California, Riverside)

CrowdGuard: Federated Backdoor Detection in Federated Learning
Phillip Rieger (Technical University of Darmstadt); Torsten Krauß (University of Würzburg); Markus Miettinen (Technical University of Darmstadt); Alexandra Dmitrienko (University of Würzburg); Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Automatic Adversarial Adaption for Stealthy Poisoning Attacks in Federated Learning
Torsten Krauß, Jan König, Alexandra Dmitrienko, Christian Kanzow (University of Würzburg)

FreqFed: A Frequency Analysis-Based Approach for Mitigating Poisoning Attacks in Federated Learning
Hossein Fereidooni, Alessandro Pegoraro, Phillip Rieger (Technical University of Darmstadt); Alexandra Dmitrienko (University of Wuerzburg); Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Session 4A: Leaks!

Acoustic Keystroke Leakage on Smart Televisions
Tejas Kannan, Synthia Qia Wang, Max Sunog (University of Chicago); Abraham Bueno de Mesquita (University of Chicago Laboratory Schools); Nick Feamster, Henry Hoffmann (University of Chicago)

IdleLeak: Exploiting Idle State Side Effects for Information Leakage
Fabian Rauscher, Andreas Kogler, Jonas Juffinger, Daniel Gruss (Graz University of Technology)

TEE-SHirT: Scalable Leakage-Free Cache Hierarchies for TEEs
Kerem Arikan, Abraham Farrell, Williams Zhang Cen, Jack McMahon, Barry Williams, Yu David Liu (Binghamton University); Nael Abu-Ghazaleh (University of California, Riverside); Dmitry Ponomarev (Binghamton University)

Exploiting Sequence Number Leakage: TCP Hijacking in NAT-Enabled Wi-Fi Networks
Yuxiang Yang, Xuewei Feng, Qi Li (Tsinghua University); Kun Sun (George Mason University); Ziqiang Wang (Southeast University); Ke Xu (Tsinghua University)

Session 4B: ML Security (1)

GNNIC: Finding Long-Lost Sibling Functions with Abstract Similarity
Qiushi Wu (University of Minnesota); Zhongshu Gu, Hani Jamjoom (IBM Research); Kangjie Lu (University of Minnesota)

Group-based Robustness: A General Framework for Customized Robustness in the Real World
Weiran Lin, Keane Lucas (Carnegie Mellon University); Neo Eyal (Tel Aviv University); Lujo Bauer (Carnegie Mellon University); Michael K. Reiter (Duke University); Mahmood Sharif (Tel Aviv University)

Experimental Analyses of the Physical Surveillance Risks in Client-Side Content Scanning
Ashish Hooda (University of Washington); Andrey Labunets (UC San Diego); Tadayoshi Kohno (University of Washington); Earlence Fernandes (UC San Diego)

Timing Channels in Adaptive Neural Networks
Ayomide Akinsanya, Tegan Brennan (Stevens Institute of Technology)

Session 4C: Secrecy and Anonymity

AnonPSI: An Anonymity Assessment Framework for PSI
Bo Jiang, Jian Du, Qiang Yan (TikTok Inc.)

Unus pro omnibus: Multi-Client Searchable Encryption via Access Control
Jiafan Wang (Data61, CSIRO); Sherman S. M. Chow (The Chinese University of Hong Kong)

Pisces: Private and Compliable Cryptocurrency Exchange
Ya-Nan Li, Tian Qiu, Qiang Tang (The University of Sydney)

Secret-Shared Shuffle with Malicious Security
Xiangfu Song (National University of Singapore); Dong Yin (Ant Group); Jianli Bai (The University of Auckland); Changyu Dong (Guangzhou University); Ee-Chien Chang (National University of Singapore)

Session 5A: Trusted Execution Environments

SENSE: Enhancing Microarchitectural Awareness for TEEs via Subscription-Based Notification
Fan Sang, Jaehyuk Lee (Georgia Institute of Technology); Xiaokuan Zhang (George Mason University); Meng Xu (University of Waterloo); Scott Constable, Yuan Xiao, Michael Steiner, Mona Vij (Intel); Taesoo Kim (Georgia Institute of Technology)

EnclaveFuzz: Finding Vulnerabilities in SGX Applications
Liheng Chen (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences; Institute for

Network Science and Cyberspace of Tsinghua University); Zheming Li, Zheyu Ma (Institute for Network Science and Cyberspace of Tsinghua University); Yuan Li (Tsinghua University); Baojian Chen (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences); Chao Zhang (Tsinghua University)

Faults in Our Bus: Novel Bus Fault Attack to Break ARM TrustZone
Nimish Mishra, Anirban Chakraborty, Debdeep Mukhopadhyay (Department of Computer Science and Engineering, IIT Kharagpur)

Session 5B: ML Attacks (1)

Parrot-Trained Adversarial Examples: Pushing the Practicality of Black-Box Audio Attacks against Speaker Recognition Models
Rui Duan (University of South Florida); Zhe Qu (Central South University); Leah Ding (American University); Yao Liu, Zhuo Lu (University of South Florida)

Attributions for ML-based ICS Anomaly Detection: From Theory to Practice
Clement Fung, Eric Zeng, Lujo Bauer (Carnegie Mellon University)

TextGuard: Provable Defense against Backdoor Attacks on Text Classification
Hengzhi Pei (UIUC); Jinyuan Jia (UIUC, Penn State); Wenbo Guo (UC Berkeley, Purdue University); Bo Li (UIUC); Dawn Song (UC Berkeley)

Session 5C: Future Cryptography

When Cryptography Needs a Hand: Practical Post-Quantum Authentication for V2V Communications
Geoff Twardokus (Rochester Institute of Technology); Nina Bindel (SandboxAQ); Hanif Rahbari (Rochester Institute of Technology); Sarah McCarthy (University of Waterloo)

HEIR: A Unified Representation for Cross-Scheme Compilation of Fully Homomorphic Computation
Song Bian, Zian Zhao, Zhou Zhang, Ran Mao (Beihang University); Kohei Suenaga (Kyoto University); Yier Jin (University of Science and Technology of China); Zhenyu Guan, Jianwei Liu (Beihang University)

Powers of Tau in Asynchrony
Sourav Das (University of Illinois at Urbana-Champaign); Zhuolun Xiang (Aptos); Ling Ren (University of Illinois at Urbana-Champaign)

Session 6A: Network Protocols

Scrappy: SeCure Rate Assuring Protocol with PrivacY
Kosei Akama (Keio University); Yoshimichi Nakatsuka (ETH Zurich); Masaaki Sato (Tokai University); Keisuke Uehara (Keio University)

Information Based Heavy Hitters for Real-Time DNS Data Exfiltration Detection
Yarin Ozery (Ben-Gurion University of the Negev, Akamai Technologies Inc.); Asaf Nadler, Asaf Shabtai (Ben-Gurion University of the Negev)

BreakSPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet
Chuhan Wang, Yasuhiro Kuranaga, Yihang Wang (Tsinghua University); Mingming Zhang (Zhongguancun Laboratory); Linkai Zheng, Xiang Li (Tsinghua University); Jianjun Chen (Tsinghua University; Zhongguancun Laboratory); Haixin Duan (Tsinghua University; Quan Cheng Lab; Zhongguancun Laboratory); Yanzhong Lin, Qingfeng Pan (Coremail Technology Co. Ltd)

Understanding Route Origin Validation (ROV) Deployment in the Real World and Why MANRS Action 1 Is Not Followed
Lancheng Qin (Tsinghua University, BNRist); Li Chen (Zhongguancun Laboratory); Dan Li (Tsinghua University, Zhongguancun Laboratory); Honglin Ye, Yutian Wang (Tsinghua University)

Session 6B: Exploitation

UntrustIDE: Exploiting Weaknesses in VS Code Extensions
Elizabeth Lin, Igibek Koishybayev, Trevor Dunlap, William Enck, Alexandros Kapravelos (North Carolina State University)

SyzBridge: Bridging the Gap in Exploitability Assessment of Linux Kernel Bugs in the Linux Ecosystem
Xiaochen Zou, Yu Hao, Zheng Zhang, Juefei Pu (UC RIverside); Weiteng Chen (Microsoft Research, Redmond); Zhiyun Qian (UC Riverside)

File Hijacking Vulnerability: The Elephant in the Room
Chendong Yu, Yang Xiao (Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences); Jie Lu (Institute of Computing Technology of the Chinese Academy of Sciences); Yuekang Li (University of New South Wales); Yeting Li (Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences); Lian Li (Institute of Computing Technology of the Chinese Academy of Sciences); Yifan Dong, Jian Wang, Jingyi Shi, Defang Bo, Wei Huo (Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences)

Phoenix: Surviving Unpatched Vulnerabilities via Accurate and Efficient Filtering of Syscall Sequences
Hugo Kermabon-Bobinnec (Concordia University); Yosr Jarraya (Ericsson Security Research); Lingyu Wang (Concordia University); Suryadipta Majumdar (Concordia University); Makan Pourzandi (Ericsson Security Research)

Session 6C: Architecture and Cybercrime

CAGE: Complementing Arm CCA with GPU Extensions
Chenxu Wang (Southern University of Science and Technology (SUSTech) and The Hong Kong Polytechnic University); Fengwei Zhang, Yunjie Deng (Southern University of Science and Technology (SUSTech)); Kevin Leach (Vanderbilt University); Jiannong Cao (The Hong Kong Polytechnic University); Zhenyu Ning (Hunan University); Shoumeng Yan, Zhengyu He (Ant Group)

Architecting Trigger-Action Platforms for Security, Performance and Functionality
Deepak Sirone Jegan (University of Wisconsin-Madison); Michael Swift (University of Wisconsin-Madison); Earlence Fernandes (UC San Diego)

Understanding and Analyzing Appraisal Systems in the Underground Marketplaces
Zhengyi Li, Xiaojing Liao (Indiana University Bloomington)

Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms
Xigao Li, Amir Rahmati, Nick Nikiforakis (Stony Brook University)

Session 7A: Blockchain Protocols

Front-running Attack in Sharded Blockchains and Fair Cross-shard Consensus
Jianting Zhang (Purdue University); Wuhui Chen, Sifu Luo (Sun Yat-sen University); Tiantian Gong (Purdue University); Zicong Hong (The Hong Kong Polytechnic University); Aniket Kate (Purdue University)

A Two-Layer Blockchain Sharding Protocol Leveraging Safety and Liveness for Enhanced Performance
Yibin Xu, Jingyi Zheng, Boris Düdder, Tijs Slaats, Yongluan Zhou (University of Copenhagen)

Secure Multiparty Computation of Threshold Signatures Made More Efficient
Harry W. H. Wong, Jack P. K. Ma, Sherman S. M. Chow (The Chinese University of Hong Kong)

Separation is Good: A Faster Order-Fairness Byzantine Consensus
Ke Mu (Southern University of Science and Technology, China); Bo Yin (Changsha University of Science and Technology, China); Alia Asheralieva (Loughborough University, UK); Xuetao Wei (Southern University of Science and Technology, China & Guangdong Provincial Key Laboratory of Brain-inspired Intelligent Computation, SUSTech, China)

Session 7B: ML Security (2)

ORL-AUDITOR: Dataset Auditing in Offline Deep Reinforcement Learning
Linkang Du (Zhejiang University); Min Chen (CISPA Helmholtz Center for Information Security); Mingyang Sun, Shouling Ji, Peng Cheng, Jiming Chen (Zhejiang University); Zhikun Zhang (Stanford University)

DRAINCLoG: Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs
Hanna Kim (KAIST); Jian Cui (Indiana University Bloomington); Eugene Jang, Chanhee Lee, Yongjae Lee, Jin-Woo Chung (S2W Inc.); Seungwon Shin (KAIST)

MPCDiff: Testing and Repairing MPC-Hardened Deep Learning Models
Qi Pang (Carnegie Mellon University); Yuanyuan Yuan (HKUST); Shuai Wang (HKUST)

K-LEAK: Towards Automating the Generation of Multi-Step Infoleak Exploits against the Linux Kernel
Zhengchuan Liang, Xiaochen Zou, Chengyu Song, Zhiyun Qian (UC Riverside)

Session 7C: Human Factors

Sharing cyber threat intelligence: Does it really help?
Beomjin Jin, Eunsoo Kim (Sungkyunkwan University); Hyunwoo Lee (KENTECH); Elisa Bertino (Purdue University); Doowon Kim (University of Tennessee, Knoxville); Hyoungshick Kim (Sungkyunkwan University)

Bernoulli Honeywords
Ke Coby Wang, Michael K. Reiter (Duke University)

Towards Automated Regulation Analysis for Effective Privacy Compliance
Sunil Manandhar, Kapil Singh (IBM T.J. Watson Research Center); Adwait Nadkarni (William & Mary)

ActiveDaemon: Unconscious DNN Dormancy and Waking Up via User-specific Invisible Token
Ge Ren, Gaolei Li, Shenghong Li, Libo Chen (Shanghai Jiao Tong University); Kui Ren (Zhejiang University)

Session 8A: Mobile Ecosystem

Maginot Line: Assessing a New Cross-app Threat to PII-as-Factor Authentication in Chinese Mobile Apps
Fannv He (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China); Yan Jia (DISSec, College of Cyber Science, Nankai University, China); Jiayu Zhao, Yue Fang, Jice Wang, Mengyue Feng (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China); Peng Liu (College of Information Sciences and Technology, Pennsylvania State University, USA); Yuqing Zhang (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China; Hangzhou Institute of Technology & School of Cyber Engineering, Xidian University, China; School of Cyberspace Security, Hainan University, China)

AAKA: An Anti-Tracking Cellular Authentication Scheme Leveraging Anonymous Credentials
Hexuan Yu, Changlai Du (Virginia Polytechnic Institute and State University); Yang Xiao (University of Kentucky); Angelos Keromytis (Georgia Institute of Technology); Chonggang Wang, Robert Gazda (InterDigital); Y. Thomas Hou, Wenjing Lou (Virginia Polytechnic Institute and State University)

5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service
Haohuang Wen (The Ohio State University); Phillip Porras, Vinod Yegneswaran, Ashish Gehani (SRI International); Zhiqiang Lin (The Ohio State University)

Leaking the Privacy of Groups and More: Understanding Privacy Risks of Cross-App Content Sharing in Mobile Ecosystem
Jiangrong Wu, Yuhong Nan (Sun Yat-sen University); Luyi Xing (Indiana University Bloomington); Jiatao Cheng (Sun Yat-sen University); Zimin Lin (Alibaba Group); Zibin Zheng (Sun Yat-sen University); Min Yang (Fudan University)

Session 8B: Acoustic Sensor Security

Detecting Voice Cloning Attacks via Timbre Watermarking
Chang Liu (University of Science and Technology of China); Jie Zhang, Tianwei Zhang (Nanyang Technological University); Xi Yang, Weiming Zhang, NengHai Yu (University of Science and Technology of China)

Eavesdropping on Black-box Mobile Devices via Audio Amplifier's EMR
Huiling Chen, Wenqiang Jin, Yupeng Hu, Zhenyu Ning (College of Computer Science and Electronic Engineering, Hunan University, Changsha, China); Kenli Li (College of Computer Science and Electronic Engineering, National Supercomputing Center in Changsha, Hunan University); Zheng Qin (College of Computer Science and Electronic Engineering, Hunan University, Changsha, China); Mingxing Duan (College of Computer Science and Electronic Engineering, National Supercomputing Center in Changsha, Hunan University); Yong Xie (Nanjing University of Posts and Telecommunications, Nanjing, China); Daibo Liu (College of Computer Science and Electronic Engineering, Hunan University, Changsha, China); Ming Li (The University of Texas at Arlington, USA)

Compensating Removed Frequency Components: Thwarting Voice Spectrum Reduction Attacks
Shu Wang, Kun Sun (George Mason University); Qi Li (Tsinghua University)

Inaudible Adversarial Perturbation: Manipulating the Recognition of User Speech in Real Time
Xinfeng Li, Chen Yan, Xuancun Lu, Zihan Zeng, Xiaoyu Ji, Wenyuan Xu (Zhejiang University)

Session 8C: Smart Contracts

Not your Type! Detecting Storage Collision Vulnerabilities in Ethereum Smart Contracts
Nicola Ruaro, Fabio Gritti, Robert McLaughlin, Ilya Grishchenko (University of California, Santa Barbara); Christopher Kruegel, Giovanni Vigna (UC Santa Barbara and VMware)

Abusing the Ethereum Smart Contract Verification Services for Fun and Profit
Pengxiang Ma (Huazhong University of Science and Technology); Ningyu He (Peking University); Yuhua Huang, Haoyu Wang (Huazhong University of Science and Technology); Xiapu Luo (The Hong Kong Polytechnic University)

Security-Performance Tradeoff in DAG-based Proof-of-Work Blockchain Protocols
Shichen Wu (1. School of Cyber Science and Technology, Shandong University 2. Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education); Puwen Wei (1. School of Cyber Science and Technology, Shandong University 2. Quancheng Laboratory 3. Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education); Ren Zhang (Cryptape Co. Ltd. and Nervos); Bowen Jiang (1. School of Cyber Science and Technology, Shandong University 2. Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education)

VETEOS: Statically Vetting EOSIO Contracts for the "Groundhog Day" Vulnerabilities
Levi Taiji Li (University of Utah); Ningyu He (Peking University); Haoyu Wang (Huazhong University of Science and Technology); Mu Zhang (University of Utah)

Session 9A: Fuzz-more-things!

DeepGo: Predictive Directed Greybox Fuzzing
Peihong Lin, Pengfei Wang, Xu Zhou, Wei Xie, Gen Zhang, Kai Lu (National University of Defense Technology)

MOCK: Optimizing Kernel Fuzzing Mutation with Context-aware Dependency
Jiacheng Xu, Xuhong Zhang, Shouling Ji (Zhejiang University); Yuan Tian (UCLA); Binbin Zhao (Georgia Institute of Technology); Qinying Wang, Peng Cheng, Jiming Chen (Zhejiang University)

Predictive Context-sensitive Fuzzing
Pietro Borrello (Sapienza University of Rome); Andrea Fioraldi (EURECOM); Daniele Cono D'Elia (Sapienza University of Rome); Davide Balzarotti (Eurecom); Leonardo Querzoni (Sapienza University of Roma); Cristiano Giuffrida (Vrije Universiteit Amsterdam)

Session 9B: ML Security (3)

Private Aggregate Queries to Untrusted Databases
Syed Mahbub Hafiz, Chitrabhanu Gupta, Warren Wnuck, Brijesh Vora, Chen-Nee Chuah (University of California, Davis)

Low-Quality Training Data Only? A Robust Framework for Detecting Encrypted Malicious Network Traffic
Yuqi Qing (Tsinghua University); Qilei Yin (Zhongguancun Laboratory); Xinhao Deng, Yihao Chen, Zhuotao Liu (Tsinghua University); Kun Sun (George Mason University); Ke Xu, Jia Zhang, Qi Li (Tsinghua University)

Don't Interrupt Me - A Large-Scale Study of On-Device Permission Prompt Quieting in Chrome
Marian Harbach, Igor Bilogrevic, Enrico Bacis, Serena Chen, Ravjit Uppal, Andy Paicu, Elias Klim, Meggyn Watkins, Balazs Engedy (Google)

Session 9C: Occlusion and Vision

DorPatch: Distributed and Occlusion-Robust Adversarial Patch to Evade Certifiable Defenses
Chaoxiang He, Xiaojing Ma (Huazhong University of Science and Technology); Bin B. Zhu (Microsoft Research); Yimiao Zeng, Hanqing Hu, Xiaofan Bai, Hai Jin (Huazhong University of Science and Technology); Dongmei Zhang (Microsoft Research)

UniID: Spoofing Face Authentication System by Universal Identity
Zhihao Wu, Yushi Cheng, Shibo Zhang, Xiaoyu Ji, Wenyuan Xu (Zhejing University)

You Can Use But Cannot Recognize: Preserving Visual Privacy in Deep Neural Networks
Qiushi Li, Yan Zhang, Ju Ren, Qi Li, Yaoxue Zhang (Tsinghua University)

Session 10A: Internet-of-Everything

From Hardware Fingerprint to Access Token: Enhancing the Authentication on IoT Devices
Yue Xiao (Wuhan University); Yi He (Tsinghua University); Xiaoli Zhang (Zhejiang University of Technology); Qian Wang (Wuhan University); Renjie Xie (Tsinghua University); Kun Sun (George Mason University); Ke Xu, Qi Li (Tsinghua University)

CP-IoT: A Cross-Platform Monitoring System for Smart Home
Hai Lin, Chenglong Li, Jiahai Yang, Zhiliang Wang (Tsinghua University); Linna Fan (National University of Defense Technology); Chenxin Duan (Tsinghua University)

Faster and Better: Detecting Vulnerabilities in Linux-based IoT Firmware with Optimized Reaching Definition Analysis
Zicong Gao (State Key Laboratory of Mathematical Engineering and Advanced Computing); Chao Zhang (Tsinghua University); Hangtian Liu (State Key Laboratory of Mathematical Engineering and Advanced Computing); Wenhou Sun (Tsinghua University); Zhizhuo Tang, Liehui Jiang (State Key Laboratory of Mathematical Engineering and Advanced Computing); Jianjun Chen (Tsinghua University); Yong Xie (Qinghai University)

Session 10B: Usable Security

The Dark Side of E-Commerce: Dropshipping Abuse as a Business Model
Arjun Arunasalam (Purdue University); Andrew Chu (University of Chicago); Muslum Ozgur Ozmen (Purdue University); Habiba Farrukh (University of California, Irvine); Z. Berkay Celik (Purdue University)

From Interaction to Independence: zkSNARKs for Transparent and Non-Interactive Remote Attestation
Shahriar Ebrahimi, Parisa Hassanizadeh (IDEAS-NCBR)

A Security and Usability Analysis of Local Attacks Against FIDO2
Tarun Kumar Yadav, Kent Seamons (Brigham Young University)

Session 10C: Membership Inference

SLMIA-SR: Speaker-Level Membership Inference Attacks against Speaker Recognition Systems
Guangke Chen (ShanghaiTech University); Yedi Zhang (National University of Singapore); Fu Song (Institute of Software, Chinese Academy of Sciences; University of Chinese Academy of Sciences)

Crafter: Facial Feature Crafting against Inversion-based Identity Theft on Deep Models
Shiming Wang, Zhe Ji, Liyao Xiang, Hao Zhang, Xinbing Wang (Shanghai Jiao Tong University); Chenghu Zhou (Chinese Academy of Sciences); Bo Li (Hong Kong University of Science and Technology)

Overconfidence is a Dangerous Thing: Mitigating Membership Inference Attacks by Enforcing Less Confident Prediction
Zitao Chen, Karthik Pattabiraman (University of British Columbia)

Session 11A: Visual Sensor Security

CamPro: Camera-based Anti-Facial Recognition
Wenjun Zhu, Yuan Sun, Jiani Liu, Yushi Cheng, Xiaoyu Ji, Wenyuan Xu (Zhejiang University)

EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras
Yan Long (University of Michigan); Qinhong Jiang, Chen Yan (Zhejiang University); Tobias Alam (University of Michigan); Xiaoyu Ji, Wenyuan Xu (Zhejiang University); Kevin Fu (Northeastern University)

Eavesdropping on Controller Acoustic Emanation for Keystroke Inference Attack in Virtual Reality
Shiqing Luo, Anh Nguyen (George Mason University); Hafsa Farooq (Georgia State University); Kun Sun, Zhisheng Yan (George Mason University)

PrintListener: Uncovering the Vulnerability of Fingerprint Authentication via the Finger Friction Sound
Man Zhou, Shuao Su (Huazhong University of Science and Technology); Qian Wang (Wuhan University); Qi Li (Tsinghua University); Yuting Zhou, Xiaojing Ma (Huazhong University of Science and Technology); Zhengxiong Li (University of Colorado Denver)

Session 11B: Reverse Engineering

SigmaDiff: Semantics-Aware Deep Graph Matching for Pseudocode Diffing
Lian Gao, Yu Qu (University of California Riverside); Sheng Yu (University of California, Riverside & Deepbits Technology Inc.); Yue Duan (Singapore Management University); Heng Yin (University of California, Riverside & Deepbits Technology Inc.)

DeGPT: Optimizing Decompiler Output with LLM
Peiwei Hu, Ruigang Liang (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China); Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences, China)

DynPRE: Protocol Reverse Engineering via Dynamic Inference
Zhengxiong Luo (Tsinghua University); Kai Liang (Central South University); Yanyang Zhao, Feifan Wu, Junze Yu (Tsinghua University); Heyuan Shi (Central South University); Yu Jiang (Tsinghua University)

Gradient Shaping: Enhancing Backdoor Attack Against Reverse Engineering
Rui Zhu (Indiana University Bloominton); Di Tang, Siyuan Tang, Zihao Wang (Indiana University Bloomington); Guanhong Tao (Purdue University); Shiqing Ma (University of Massachusetts Amherst); XiaoFeng Wang (Indiana University Bloomington); Haixu Tang (Indiana University, Bloomington)

Session 11C: Prompt Engineering

MASTERKEY: Automated Jailbreaking of Large Language Model Chatbots
Gelei Deng, Yi Liu (Nanyang Technological University); Yuekang Li (University of New South Wales); Kailong Wang (Huazhong University of Science and Technology); Ying Zhang (Virginia Tech); Zefeng Li (Nanyang Technological University); Haoyu Wang (Huazhong University of Science and Technology); Tianwei Zhang, Yang Liu (Nanyang Technological University)

LMSanitator: Defending Prompt-Tuning Against Task-Agnostic Backdoors
Chengkun Wei, Wenlong Meng (Zhejiang University); Zhikun Zhang (Stanford University); Min Chen (CISPA Helmholtz Center for Information Security); Minghu Zhao (Zhejiang University); Wenjing Fang, Lei Wang (Ant Group); Zihui Zhang, Wenzhi Chen (Zhejiang University)

Improving the Robustness of Transformer-based Large Language Models with Dynamic Attention
Lujia Shen, Yuwen Pu, Shouling Ji (Zhejiang University); Changjiang Li (Penn State); Xuhong Zhang (Zhejiang University); Chunpeng Ge (Shandong University); Ting Wang (Penn State)

DEMASQ: Unmasking the ChatGPT Wordsmith
Kavita Kumari (Technical University of Darmstadt); Alessandro Pegoraro, Hossein Fereidooni, Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Session 12A: Network Security

IDA: Hybrid Attestation with Support for Interrupts and TOCTOU
Fatemeh Arkannezhad, Justin Feng, Nader Sehatbakhsh (UCLA)

LoRDMA: A New Low-Rate DoS Attack in RDMA Networks
Shicheng Wang (Tsinghua University); Menghao Zhang (Beihang University & Infrawaves); Yuying Du (Information Engineering University); Ziteng Chen (Southeast University); Zhiliang Wang, Mingwei Xu (Tsinghua University & Zhongguancun Laboratory); Renjie Xie (Tsinghua University); Jiahai Yang (Tsinghua University & Zhongguancun Laboratory)

PriSrv: Privacy-Enhanced and Highly Usable Service Discovery in Wireless Communications
Yang Yang, Robert H. Deng, Guomin Yang (School of Computing and Information Systems, Singapore Management University, Singapore); Yingjiu Li (Department of Computer Science, University of Oregon, USA); HweeHwa Pang, Minming Huang (School of Computing and Information Systems, Singapore Management University, Singapore); Rui Shi (School of Cyberspace Security, Beijing University

of Posts and Telecommunications, Beijing, China); Jian Weng (College of Information Science and Technology, Jinan University, Guangzhou, China)

NODLINK: An Online System for Fine-Grained APT Attack Detection and Investigation
Shaofei Li (Key Laboratory of High-Confidence Software Technologies (MOE), School of Computer Science, Peking University); Feng Dong (Huazhong University of Science and Technology); Xusheng Xiao (Arizona State University); Haoyu Wang (Huazhong University of Science and Technology); Fei Shao (Case Western Reserve University); Jiedong Chen (Sangfor Technologies Inc.); Yao Guo, Xiangqun Chen (Key Laboratory of High-Confidence Software Technologies (MOE), School of Computer Science, Peking University); Ding Li (Key Laboratory of High-Confidence Software Technologies (MOE), School of Computer Science, Peking University)

Session 12B: Application Security

ReplicaWatcher: Training-less Anomaly Detection in Containerized Microservices
Asbat El Khairi (University of Twente); Marco Caselli (Siemens AG); Andreas Peter (University of Oldenburg); Andrea Continella (University of Twente)

TALISMAN: Tamper Analysis for Reference Monitors
Frank Capobianco, Quan Zhou, Aditya Basu (The Pennsylvania State University); Trent Jaeger (The Pennsylvania State University, University of California, Riverside); Danfeng Zhang (The Pennsylvania State University, Duke University)

BliMe: Verifiably Secure Outsourced Computation with Hardware-Enforced Taint Tracking
Hossam ElAtali (University of Waterloo); Lachlan J. Gunn (Aalto University); Hans Liljestrand (University of Waterloo); N. Asokan (University of Waterloo, Aalto University)

Efficient Use-After-Free Prevention with Opportunistic Page-Level Sweeping
Chanyoung Park, Hyungon Moon (UNIST)

Session 12C: Automotive Sensor Security

GhostType: The Limits of Using Contactless Electromagnetic Interference to Inject Phantom Keys into Analog Circuits of Keyboards
Qinhong Jiang, Yanze Ren (Zhejiang University); Yan Long (University of Michigan); Chen Yan (Zhejiang University); Yumai Sun (University of Michigan); Xiaoyu Ji (Zhejiang University); Kevin Fu (Northeastern University); Wenyuan Xu (Zhejiang University)

LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies
Takami Sato (University of California, Irvine); Yuki Hayakawa, Ryo Suzuki, Yohsuke Shiiki, Kentaro Yoshioka (Keio University); Qi Alfred Chen (University of California, Irvine)

Invisible Reflections: Leveraging Infrared Laser Reflections to Target Traffic Sign Perception
Takami Sato (University of California Irvine); Sri Hrushikesh Varma Bhupathiraju (University of Florida); Michael Clifford (Toyota InfoTech Labs); Takeshi Sugawara (The University of Electro-Communications); Qi Alfred Chen (University of California, Irvine); Sara Rampazzi (University of Florida)

MadRadar: A Black-Box Physical Layer Attack Framework on mmWave Automotive FMCW Radars
David Hunt, Kristen Angell, Zhenzhou Qi, Tingjun Chen, Miroslav Pajic (Duke University)

Session 13A: Web Security

Untangle: Multi-Layer Web Server Fingerprinting
Cem Topcuoglu (Northeastern University); Kaan Onarlioglu (Akamai Technologies); Bahruz Jabiyev, Engin Kirda (Northeastern University)

Certificate Transparency Revisited: The Public Inspections on Third-party MonitorsAozhuo Sun (Institute of Information Engineering, Chinese Academy of Sciences); Jingqiang Lin (School of Cyber Science and Technology, University of Science and Technology of China); Wei Wang (Institute of Information Engineering, Chinese Academy of Sciences); Zeyan Liu (The University of Kansas); Bingyu Li (School of Cyber Science and Technology, Beihang University); Shushang Wen (School of Cyber Science and Technology, University of Science and Technology of China); Qiongxiao Wang (BeiJing Certificate Authority Co., Ltd.); Fengjun Li (The University of Kansas)

Compromising Industrial Processes using Web-Based Programmable Logic Controller Malware
Ryan Pickren, Tohid Shekari, Saman Zonouz, Raheem Beyah (Georgia Institute of Technology)

TrustSketch: Trustworthy Sketch-based Telemetry on Cloud Hosts
Zhuo Cheng (Carnegie Mellon University); Maria Apostolaki (Princeton University); Zaoxing Liu (University of Maryland); Vyas Sekar (Carnegie Mellon University)

Session 13B: ML Attacks (2)

Transpose Attack: Stealing Datasets with Bidirectional Training
Guy Amit, Moshe Levy, Yisroel Mirsky (Ben-Gurion University)

Sneaky Spikes: Uncovering Stealthy Backdoor Attacks in Spiking Neural Networks with Neuromorphic Data
Gorka Abad (Radboud University & Ikerlan Technology Research Centre); Oğuzhan Ersoy (Radboud University); Stjepan Picek (Radboud University & Delft University of Technology); Aitor Urbieta (Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA))

GraphGuard: Detecting and Counteracting Training Data Misuse in Graph Neural Networks
Bang Wu (CSIRO's Data61/Monash University); He Zhang, Xiangwen Yang (Monash University); Shuo Wang (CSIRO's Data61/Shanghai Jiao Tong University); Minhui Xue (CSIRO's Data61); Shirui Pan (Griffith University); Xingliang Yuan (Monash University)

Enhance Stealthiness and Transferability of Adversarial Attacks with Class Activation Mapping Ensemble Attack
Hui Xia, Rui Zhang, Zi Kang, Shuliang Jiang, Shuo Xu (Ocean University of China)

Session 13C: ML Privacy

A Duty to Forget, a Right to be Assured? Exposing Vulnerabilities in Machine Unlearning Services
Hongsheng Hu, Shuo Wang (CSIRO's Data61); Jiamin Chang, Haonan Zhong (University of New South Wales); Ruoxi Sun (CSIRO's Data61); Shuang Hao (University of Texas at Dallas); Haojin Zhu (Shanghai Jiao Tong University); Minhui Xue (CSIRO's Data61)

Pencil: Private and Extensible Collaborative Learning without the Non-Colluding Assumption
Xuanqi Liu, Zhuotao Liu, Qi Li, Ke Xu, Mingwei Xu (Tsinghua University)

SSL-WM: A Black-Box Watermarking Approach for Encoders Pre-trained by Self-Supervised Learning
Peizhuo Lv, Pan Li, Shenchen Zhu (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); Kai Chen, Ruigang Liang, Chang Yue, Fang Xiang, Yuling Cai, Hualong Ma (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China); Yingjun Zhang (Institute of Software, Chinese Academy of Sciences, China); Guozhu Meng (Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China)

Message from the General Chairs

Welcome to the 2024 Network and Distributed System Security (NDSS) Symposium! The organizing and technical program committee put together an attractive program which includes 140 papers and 2 keynotes from Meredith Whittaker, President of Signal Foundation and Herbert Bos, Professor at Vrije Universiteit Amsterdam, along with 8 co-hosted events, birds-of-a-feather sessions, and a poster session.

A program like this could not be organized without the tireless efforts from a large number of volunteers, and they all deserve a huge amount of thanks. First, we would like to thank the Technical Program Committee Co-Chairs, Mathias Payer and Christina Pöpper, who have put together a great program. NDSS 2024 had two submission phases, and thanks goes to the program committee members, and the external reviewers for their work in reviewing paper submissions, shepherding the through major and minor revisions, and selecting the best papers to be presented. A special thanks also goes to David Balenson and Mridula Singh as publications chairs for collecting the camera-ready papers and ensuring they are published.

We would like to also thank Xiajing Liao and Jelena Mirkovic for selecting a dynamic set of co-located events. This year NDSS will host:

1) Vehicle Security and Privacy (VehicleSec);
2) Binary Analysis Research (BAR);
3) Artificial Intelligence System with Confidential Computing (AISCC);
4) Security and Privacy in Standardized IoT (SDIoTSec);
5) Measurements, Attacks, and Defenses for the Web (MADWeb);
6) Security of Space and Satellite Systems (SpaceSec);
7) Security Operation Center Operations and Construction (WOSOC); and
8) Usable Security and Privacy (USEC).

There are many other people who have helped make NDSS 2024 a success, and we would like to thank Tiffany Bao and Tianshi Li for coordinating a wonderful poster session this year, including organizing the best poster awards. We would also like to thank Sara Rampazzi and her team for reviewing the student grant applications (31 students received travel grants this year), Ramjita Pai Kasturi for publicity, Tom Hutton as local arrangements chair. Finally, the Steering Group deserves thanks for their active participation and wise advice.

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, Ant Group, TikTok, Google, FutureWei, IBM, and Qualcomm. Thank you to Colorado State University and CyberTruck Challenge for sponsoring the reception and to NSF and ONR for funding student travel grants. VehicleSec is sponsored by Denso, ETAS, GM, NMFTA, Zoom, ASU and ST Microelectronics.

NDSS would not happen if it were not for the incredible support from Karen O’Donoghue, Robin Wilton, Joseph Lorenzo Hall and their team – thank you!! And thank you to the Internet Society for their continued support of NDSS, 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 your support building a warm community around this symposium. We hope that you enjoy NDSS 2024!

Cristina Nita-Rotaru and Yongdae Kim
General Chairs, NDSS 2024

Message from the Program Committee Co-Chairs

It is our great pleasure to present to you the technical program of the 2024 Network and Distributed System Security (NDSS) symposium, held between February 26 and March 1, 2024. For the past 31 years, NDSS has established itself as one of the top conferences in systems 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 682 complete submissions over two submission cycles (i.e., not counting 13 desk-rejected papers that clearly violated the submission guidelines), an increase of 108 papers compared to the previous year. 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, 140 papers (at a20.5% 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, possibly in a minor or major revision process. Each paper received two initial reviews and, if either review identified positive feedback it advanced to the second round of reviewing. 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 2024. General Chairs Cristina Nita-Rotaru and Joseph Lorenzo Hall oversaw the conference and worked closely with us. Robin Wilton served as a critical interface between the Program Co-Chairs, the Organizing Committee, and ISOC. Publicity Chair Reethika Ramesh worked seamlessly with us to solicit submissions and promote the conference. Publications Co-Chairs David Balenson and Mridula Singh took excellent care of the proceedings production matters. Artifact evaluation chair Daniele Cono D’Elia did an amazing job of juggling tight deadlines and ensuring successful evaluation of the submitted artifacts. Finally, we thank Meredith Whittaker and Herbert Bos for giving the keynotes at this year’s symposium.

Lastly, we would like to thank our 116 PC members and the three external reviewers. As reviewers and shepherds, 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 2024 and all attendees who are joining us at NDSS 2024, without whom NDSS would not be possible. Enjoy the conference!

Mathias Payer and Christina Pöpper
Program Committee Co-Chairs, NDSS 2024

Message from the Internet Society

The Internet Society is proud to host the Network and Distributed System Security (NDSS) Symposium 2024, continuing our involvement with NDSS throughout its life and evolution to date. NDSS's position as a leading global conference for computer and network security research is a testament to the recognition it has earned from the research community both in academia and industry.

The Internet Society's mission of an open, globally connected, secure and trustworthy Internet depends on the work you do here. Your focus on high-quality peer-reviewed research, and on fostering the next generation of leaders in security and privacy, raises the bar for computer and network security. That leads to better technology, more secure deployment, and ultimately, a more trustworthy Internet. Thank you.

For 2024, NDSS returns to a fully in-person. five-day format. As you have heard from the General Chairs, NDSS 2024 has attracted eight co-located events, including familiar topics like vehicle security, usable security and privacy, and an inevitable but welcome new entry – AISCC (Artificial Intelligence Systems with Confidential Computing).

This year the Program Committee received almost 600 submissions, from which they have created a packed program of 140 paper presentations. We're also very pleased to welcome two world-class keynote speakers, in Meredith Whittaker (President of Signal) and Professor Herbert Bos (Vrije Universiteit Amsterdam).

NDSS relies 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 Cristina Nita-Rotaru and Joseph Lorenzo Hall, Program Committee Co-Chairs Mathias Payer and Christina Pöpper, and the many other members of the Organizing and Program Committees who have invested countless hours to review papers and posters, organize the co-located sessions, publicize the event, and publish the proceedings.

Finally, I am profoundly grateful to the sponsors without whom this event would not be possible. This includes our Patron Sponsor Ant Group; Gold Sponsors Google and TikTok; Silver Sponsors FutureWei and IBM; and our lanyard sponsor Qualcomm. The NDSS-VehicleSec Reception is kindly sponsored by CSU and the CyberTruck Challenge.

Some of you are here thanks to student support grants from the ONR and the NSF, and I would like to thank them for their generosity. I hope you will take the opportunity to meet the NSF's Secure and Trustworthy Cyberspace (S&TC) team while you are at NDSS.

Thank you, also, to our co-located event sponsors: Arizona State University, Denso, ETAS, General Motors, the National Motor Freight Traffic Association (NMFTA), Zoox, and ST Microelectronics.

On behalf of the Internet Society, I welcome you to NDSS 2024. Your week is going to be a full one: I hope it is also productive and fun.

Andrew Sullivan
CEO, Internet Society

Program Committee

Mathias Payer, *EPFL* (Co-Chair)
Christina Pöpper, *New York University Abu Dhabi* (Co-Chair)

Aanjhan Ranganathan, *Northeastern University*
Adrian Dabrowski, *CISPA Helmholtz Center for Information Security*
Adwait Nadkarni, *William & Mary*
Ahmad-Reza Sadeghi, *Technical University of Darmstadt*
Alessandro Sorniotti, *IBM Research – Europe*
Alexandra Dmitrienko, *University of Würzburg*
Alvaro Cardenas, *University of California, Santa Cruz*
Amir Rahmati, *Stony Brook University*
Aravind Machiry, *Purdue University*
Bart Coppens, *Ghent University*
Ben Stock, *CISPA Helmholtz Center for Information Security*
Benjamin Andow, *Google*
Bo Feng, *Georgia Institute of Technology*
Boris Köpf, *Azure Research*
Brendan Saltaformaggio, *Georgia Institute of Technology*
Christophe Hauser, *Dartmouth College*
Christopher Kruegel, *UC Santa Barbara*
Christopher Liebchen, *Google*
Daniel Gruss, *Graz University of Technology*
Daniele Antonioli, *EURECOM*
Daniele Cono D'Elia, *Sapienza University of Rome*
Dave (Jing) Tian, *Purdue University*
Ding Wang, *Nankai University*
Dipanjan Das, *University of California, Santa Barbara*
Doowon Kim, *University of Tennessee, Knoxville*
Eleonora Losiouk, *University of Padua*
Erik van der Kouwe, *Vrije Universiteit Amsterdam*
Fengwei Zhang, *Southern University of Science and Technology*
Flavio Toffalini, *EPFL*
Gang Wang, *University of Illinois at Urbana-Champaign*
Ghassan Karame, *Ruhr-University Bochum*
Gianluca Stringhini, *Boston University*
Giovanni Apruzzese, *University of Liechtenstein*
Guangdong Bai, *The University of Queensland*
Güliz Seray Tuncay, *Google*
Guofei Gu, *Texas A&M University*
Habiba Farrukh, *Purdue University*
Haibin Zhang, *Beijing Institute of Technology*

Haipeng Cai, *Washington State University*
Hamed Okhravi, *MIT Lincoln Laboratory*
Haojin Zhu, *Shanghai Jiao Tong University*
Hong Hu, *Pennsylvania State University*
Hossein Fereidooni, *Technical University of Darmstadt*
Houman Homayoun, *University of California Davis*
Imtiaz Karim, *Purdue University*
Insu Yun, *KAIST*
Jason (Minhui) Xue, *CSIRO's Data61*
Johanna Sepúlveda, *Airbus Defence and Space*
Jun Xu, *University of Utah*
Juraj Somorovsky, *Paderborn University*
Kangjie Lu, *University of Minnesota*
Katerina Mitrokotsa, *University of St. Gallen*
Kun Sun, *George Mason University*
Lannan Luo, *George Mason University*
Lejla Batina, *Radboud University*
Lorenzo Cavallaro, *University College London*
Luca Mariot, *University of Twente*
Manuel Egele, *Boston University*
Marcus Botacin, *Texas A&M University*
Marcus Peinado, *Microsoft Research*
Martin Henze, *RWTH Aachen University & Fraunhofer FKIE*
Mathy Vanhoef, *KU Leuven*
Meng Luo, *Zhejiang University*
Meng Xu, *University of Waterloo*
Merve Sahin, *SAP Security Research*
Michael Schwarz, *CISPA Helmholtz Center for Information Security*
Mihalis Maniatakos, *New York University Abu Dhabi*
Min Suk Kang, *KAIST*
Ming Li, *The University of Texas at Arlington*
Mitsuaki Akiyama, *NTT*
Mridula Singh, *CISPA Helmholtz Center for Information Security*
Mu Zhang, *University of Utah*
Nathan Burow, *MIT Lincoln Laboratory*
Neil Gong, *Duke University*
Nick Sullivan, *Cloudflare Inc.*
Norrathep Rattanavipanon, *Prince of Songkla University*
Omar Chowdhury, *Stony Brook University*
Phani Vadrevu, *University of New Orleans*
Qi Li, *Tsinghua University*
Qiang Tang, *The University of Sydney*
Ren Zhang, *Cryptape Co. Ltd. and Nervos*

René Mayrhofer, *JKU Linz*
Saman Zonouz, *Georgia Institute of Technology*
Samuel Jero, *MIT Lincoln Laboratory*
Sandra Siby, *Imperial College London*
Sang Kil Cha, *KAIST*
Sanghyun Hong, *Oregon State University*
Sarah Zennou, *Airbus*
Shagufta Mehnaz, *Pennsylvania State University*
Sherman S. M. Chow, *Chinese University of Hong Kong*
Sisi Duan, *Tsinghua University*
Srdjan Capkun, *ETH Zurich*
Stefan Brunthaler, *μCSRL, University of the Bundeswehr Munich*
Stjepan Picek, *Radboud University*
Syed Rafiul Hussain, *Pennsylvania State University*
Takuya Watanabe, *NTT*
Theodor Schnitzler, *TU Dortmund*
Tianhao Wang, *University of Virginia*
Ting Chen, *University of Electronic Science and Technology of China*
Trent Jaeger, *Pennsylvania State University*
Tuba Yavuz, *University of Florida*
Vasileios Kemerlis, *Brown University*
Wenke Lee, *Georgia Institute of Technology*
Xiaoyu Ji, *Zhejiang University*
Xiapu Luo, *The Hong Kong Polytechnic University*
Xinyang Ge, *Databricks*
Yanjiao Chen, *Zhejiang University*
Yongdae Kim, *KAIST*
Yuan Zhang, *Fudan University*
Yue Zhang, *The Ohio State University*
Yuseok Jeon, *UNIST*
Yuzhe Tang, *Syracuse University*
Z. Berkay Celik, *Purdue University*
Zhikun Zhang, *CISPA Helmholtz Center for Information Security and Stanford University*
Zhou Li, *University of California, Irvine*

External Reviewers

Amit Seal Ami, *William & Mary*
Andreas Kogler, *Graz University of Technology*
Ao Zhang, *Tsinghua University*
Behrad Tajalli, *Radboud University*
Beomseok Oh, *KAIST*
Chenyu Li, *University of Chinese Academy of Sciences*
Cheoljun Park, *KAIST*
Christoforos Vasilatos, *New York University Abu Dhabi*
Chuanpu Fu, *Tsinghua University*
Chuxiong Wu, *George Mason University*
Constantine Doumanidis, *New York University Abu Dhabi*
Daniel Arp, *TU Berlin*
Dohyun Kim, *KAIST*
Dunia Mahboobeh, *New York University Abu Dhabi*
Efren Lopez, *Texas A&M Corpus Christi*
Fabian Rauscher, *Graz University of Technology*
Feargus Pendlebury, *Meta*
Feiyang Qiu, *KU Leuven*
Gorka Abad, *Radboud University and Ikerlan Research Center*
Haeun Lee, *KAIST*
Hanwen Feng, *University of Sydney*
Hengkai Ye, *Penn State University*
Homer Gamil, *New York University Abu Dhabi*
Huancheng Zhou, *Texas A&M University*
Ioannis Angelakopoulos, *Boston University*
Jack P. K. Ma, *Chinese University of Hong Kong*
Jaehoon Kim, *KAIST*
Jiacen Xu, *University of California, Irvine*
Jiafan Wang, *CSIRO's Data61*
Jianwei Huang, *Texas A&M University*
Jing Xu, *Delft University of Technology*
Jingwei Jiang, *Harbin Engineering University*
Jinseob Jeong, *KAIST*
Joann Qiongna Chen, *University of California, Irvine*
Johannes Ottenhues, *University of St. Gallen*
Jonas Juffinger, *Graz University of Technology*
Jost Rossel, *Paderborn University*
JungHyun Kim, *KAIST*
Junha Jang, *KAIST*
Junho Ahn, *KAIST*
Kaushal Kafle, *William & Mary*
Kevin Hong, *Texas A&M University*

Limin Yang, *TikTok*
Lucien K. L. Ng, *Georgia Institute of Technology*
Luis Burbano, *UC Santa Cruz*
Lukas Giner, *Graz University of Technology*
Manaar Alam, *New York University Abu Dhabi*
Mangi Cho, *KAIST*
Mingfei Zhang, *Shandong University*
Minxin Du, *Chinese University of Hong Kong*
Mohammad Naseri, *University College London*
Mohammed Nabeel, *New York University Abu Dhabi*
Nan Cheng, *University of St. Gallen*
Niklas Niere, *Paderborn University*
Novak Kaluderovic, *University of St. Gallen*
Oleg Mazonka, *New York University Abu Dhabi*
Peiyang Li, *Tsinghua University*
Riccardo Cestaro, *University of Padua*
Rujia Li, *Tsinghua University*
Samuele Doria, *University of Padua*
Sangdon Park, *Postech*
Sangwook Bae, *KAIST*
Shiyu Sun, *George Mason University*
Shu Wang, *George Mason University*
Shuangpeng Bai, *Penn State University*
Simeone Pizzi, *University of Padua*
Simone Zerbini, *University of Padua*
Song Liu, *Penn State University*
Soomin Kim, *KAIST*
Stefan Gast, *Graz University of Technology*
Takayuki Miura, *NTT*
Tapas Pal, *Karlsruhe Institute of Technology*
Tian Qiu, *University of Sydney*
Tianyu Cui, *Zhongguancun Laboratory*
Tuan Hoang Dinh, *KAIST*
Uddipana Dowerah, *University of St. Gallen*
Wei-Cheng Wu, *Dartmouth College*
Wen Li, *Washington State University*
Weonji Choi, *KAIST*
Xiao Sui, *Shandong University*
Xiaoyun Xu, *Radboud University*
Xin Wang, *Tsinghua University*
Xinhao Deng, *Tsinghua University*
Xu He, *George Mason University*
Xuanji Meng, *Tsinghua University*
Xuesong Bai, *University of California, Irvine*

Yanan Li, *University of Sydney*
Yu Liang, *Penn State University*
Yue Wang, *New York University Abu Dhabi*
Yuncong Zhang, *Shanghai Jiao Tong University*
Yunkai Zou, *Nankai University*
Yunlong Xing, *George Mason University*
Yunwen Liu, *Cryptape Co. Ltd.*
Yupeng Liu, *Tsinghua University*
Zengpeng Li, *Shandong University*
Zhechang Zhang, *Penn State University*
Zhenliang Lu, *University of Sydney*
Zhenzhuo Hou, *Peking University*
Zhichun Lu, *Cryptape Co. Ltd.*

Organizing Committee

General Chairs

Cristina Nita-Rotaru
Northeastern University

Yongdae Kim
KAIST

Program Committee Co-Chairs

Mathias Payer
EPFL

Christina Pöpper
New York University Abu Dhabi

Workshop Chairs

Xiaojing Liao
Indiana University

Jelena Mirkovic
USC Information Sciences Institute

Poster Session Chairs

Tianshi Li
UC Berkeley

Tiffany Bao
Arizona State University

Test of Time Award Committee

Mike Reiter (Chair)
Duke University

Ali Abbasi
CISPA Helmholtz Center

Alina Oprea
Northeastern University

Lorenzo Cavallaro
University College London

Rei Safavi-Naini
University of Calgary

Yinqian Zhang
Southern University of Science and Technology

Student Support Committee

Sara Rampazzi (Chair)
University of Florida

Xiali Hei
University of Louisiana at Lafayette

Di Ma
University Michigan – Dearborn

Nidhi Rastogi
Rochester Institute of Technology

Foteini Baldimsti
George Mason University

Marco Squarcina
TU Wien

Yuval Yarom
Ruhr University Bochum

Publicity Chair

Reethika Ramesh
University of Michigan

Artifact Evaluation Chair

Daniele Cono D’Elia
Sapienza University, Rome

Publications Chairs

David Balenson
USC Information Sciences Institute

Mridula Singh
CISPA

Local Arrangements Chair

Thomas Hutton
San Diego Supercomputer Center

Steering Group

Co-Chairs

Joseph Lorenzo Hall
Internet Society

Cristina Nita-Rotaru
Northeastern University

Steering Group Members

Yondae Kim, ex-officio
KAIST

Mathia Payer, ex-officio
EPFL

Christina Pöpper, ex-officio
New York University Abu Dhabi

Carrie Gates, ex-officio
Bank of America

David Balenson, Historian
USC Information Sciences Institute

Thomas Hutton, Local Arrangements
University of Texas San Antonio

Anita Nikolich
University of Illinois

Christopher Kruegel
University of California, Santa Barbara

Daphne Yao
Virginia Tech University

Deborah Shands
SRI International

Lorenzo Cavalaro
University College London

Gabriela Ciocarlie
University of Texas at San Antonio

Zhenkai Liang
National University of Singapore

Ahmad-Reza Sadeghi
Technical University of Darmstadt

Gene Tsudik
UC Irvine