Proceedings

2025

Network and Distributed System Security Symposium

NDSS

SYMPOSIUM/2025

Proceedings

2025

Network and Distributed System Security Symposium

February 24 – February 28, 2025

San Diego, CA, USA

Hosted by the
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) : 979-8-9894372-8-3

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

Session 1A: WiFi and Bluetooth Security "Unplugging the Hackers from Your WiFi"

Session 1B: Internet Security "Surfing the Web Safely: Don't Let the Sharks Bite"

Session 1C: Privacy & Usability 1 “Privacy That Doesn’t Hurt to Use”

Session 1D: System-Level Security “The Fortress: Securing Systems from the Inside Out”

Minnesota), Qingkai Zeng (State Key Laboratory for Novel Software Technology, Nanjing University), Kangjie Lu (University of Minnesota)

Statically Discover Cross-Entry Use-After-Free Vulnerabilities in the Linux Kernel
Hang Zhang (Indiana University Bloomington), Jangha Kim (The Affiliated Institute of ETRI, ROK), Chuhong Yuan (Georgia Institute of Technology), Zhiyun Qian (University of California, Riverside), Taesoo Kim (Georgia Institute of Technology)

VulShield: Protecting Vulnerable Code Before Deploying Patches
Yuan Li (Zhongguancun Laboratory & Tsinghua University), Chao Zhang (Tsinghua University & JCSS & Zhongguancun Laboratory), Jinhao Zhu (UC Berkeley), Penghui Li (Zhongguancun Laboratory), Chenyang Li (Peking University), Songtao Yang (Zhongguancun Laboratory), Wende Tan (Tsinghua University)

Oreo: Protecting ASLR Against Microarchitectural Attacks
Shixin Song (Massachusetts Institute of Technology), Joseph Zhang (Massachusetts Institute of Technology), Mengjia Yan (Massachusetts Institute of Technology)

Session 2A: LLM Security “When LLMs Go Rogue: Defending the Models that Write Your Emails”

The Philosopher’s Stone: Trojaning Plugins of Large Language Models
Tian Dong (Shanghai Jiao Tong University), Minhui Xue (CSIRO's Data61), Guoxing Chen (Shanghai Jiao Tong University), Rayne Holland (CSIRO's Data61), Yan Meng (Shanghai Jiao Tong University), Shaofeng Li (Southeast University), Zhen Liu (Shanghai Jiao Tong University), Haojin Zhu (Shanghai Jiao Tong University)

Safety Misalignment Against Large Language Models
Yichen Gong (Tsinghua University), Delong Ran (Tsinghua University), Xinlei He (Hong Kong University of Science and Technology (Guangzhou)), Tianshuo Cong (Tsinghua University), Anyu Wang (Tsinghua University), Xiaoyun Wang (Tsinghua University)

I know what you MEME! Understanding and Detecting Harmful Memes with Multimodal Large Language Models
Yong Zhuang (Wuhan University), Keyan Guo (University at Buffalo), Juan Wang (Wuhan University), Yiheng Jing (Wuhan University), Xiaoyang Xu (Wuhan University), Wenzhe Yi (Wuhan University), Mengda Yang (Wuhan University), Bo Zhao (Wuhan University), Hongxin Hu (University at Buffalo)

Session 2B: Web Security “Keeping the Web Safe from the Bad Guys”

The (Un)usual Suspects – Studying Reasons for Lacking Updates in WordPress
Maria Hellenthal (CISPA Helmholtz Center for Information Security), Lena Gotsche (CISPA Helmholtz Center for Information Security), Rafael Mrowczynski (CISPA Helmholtz Center for Information Security), Sarah Kugel (Saarland

Session 2C: Phishing & Fraud 1 “Hook, Line, and Cyber Sink: The Art of Phishing”

Session 2D: Android Security 1 “Bugging Android: The Chase for the Holy APK”

Session 3A: Network Security 1 “The Internet's Secret Service: Securing the Pipes”

Session 3B: Wireless, Cellular & Satellite Security “The Sky’s the Limit: Securing the Wireless Frontier”

Session 3C: Mobile Security "Mobile Security: Not Just for Your Mom's iPhone"

Session 3D: AI Safety “When Your AI Starts Watching you Back”

Session 4A: IoT Security “When Your Smart Fridge Knows Too Much”

Laboratory of Information Security), Yishun Zeng (Institute for Network Sciences and Cyberspace (INSC), Tsinghua University), Zhiyuan Jiang (National University of Defense Technology), Jiahai Yang (Institute for Network Sciences and Cyberspace (INSC), Tsinghua University)

Hidden and Lost Control: on Security Design Risks in IoT User-Facing Matter Controller
Haoqiang Wang, Yiwei Fang (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences; Indiana University Bloomington), Yichen Liu (Indiana University Bloomington), Ze Jin (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences; Indiana University Bloomington), Emma Delph (Indiana University Bloomington), Xiaojiang Du (Stevens Institute of Technology), Qixu Liu (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences), Luyi Xing (Indiana University Bloomington)

Evaluating Machine Learning-Based IoT Device Identification Models for Security Applications
Eman Maali (Imperial College London), Omar Alrawi (Georgia Institute of Technology), Julie McCann (Imperial College London)

Session 4B: Audio Security “Not Your Average Earworm: Securing the Soundwaves”

VoiceRadar: Voice Deepfake Detection using Micro-Frequency and Compositional Analysis
Kavita Kumari (Technical University of Darmstadt), Maryam Abbasihafshejani (University of Texas at San Antonio), Alessandro Pegoraro (Technical University of Darmstadt), Phillip Rieger (Technical University of Darmstadt), Kamyar Arshi (Technical University of Darmstadt), Murtuza Jadliwala (University of Texas at San Antonio), Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Characterizing the Impact of Audio Deepfakes in the Presence of Cochlear Implant
Magdalena Pasternak (University of Florida), Kevin Warren (University of Florida), Daniel Olszewski (University of Florida), Susan Nittrouer (University of Florida), Patrick Traynor (University of Florida), Kevin Butler (University of Florida)

SongBsAb: A Dual Prevention Approach against Singing Voice Conversion based Illegal Song Covers
Guangke Chen (Pengcheng Laboratory), Yedi Zhang (National University of Singapore), Fu Song (Key Laboratory of System Software (Chinese Academy of Sciences) and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Science; Nanjing Institute of Software Technology), Ting Wang (Stony Brook University), Xiaoning Du (Monash University), Yang Liu (Nanyang Technological University)

Speak Up, I’m Listening: Extracting Speech from Zero-Permission VR Sensors
Derin Cayir (Florida International University), Reham Mohamed Aburas (American University of Sharjah), Riccardo Lazzeretti (Sapienza University of Rome), Marco Angelini (Link Campus University of Rome), Abbas Acar (Florida

International University), Mauro Conti (University of Padua), Z. Berkay Celik (Purdue University), Selcuk Uluagac (Florida International University)

Session 4C: Privacy & Cryptography 1 “Breaking Ciphers, Not Trust”

Secure Transformer Inference Made Non-interactive
Jiawen Zhang (Zhejiang University), Xinpeng Yang (Zhejiang University), Lipeng He (University of Waterloo), Kejia Chen (Zhejiang University), Wen-jie Lu (Zhejiang University), Yinghao Wang (Zhejiang University), Xiaoyang Hou (Zhejiang University), Jian Liu (Zhejiang University), Kui Ren (Zhejiang University), Xiaohu Yang (Zhejiang University)

Revisiting EM-based Estimation for Locally Differentially Private Protocols
Yutong Ye (Institute of software, Chinese Academy of Sciences & Zhongguancun Laboratory, Beijing, PR.China.), Tianhao Wang (University of Virginia), Min Zhang (Institute of Software, Chinese Academy of Sciences), Dengguo Feng (Institute of Software, Chinese Academy of Sciences)

BumbleBee: Secure Two-party Inference Framework for Large Transformers
Wen-jie Lu (Ant Group), Zhicong Huang (Ant Group), Zhen Gu (Alibaba Group), Jingyu Li (Ant Group & Zhejiang University), Jian Liu (Zhejiang University), Cheng Hong (Ant Group), Kui Ren (Zhejiang University), Tao Wei (Ant Group), WenGuang Chen (Ant Group)

Repurposing Neural Networks for Efficient Cryptographic Computation
Ohio State University), Shiqing Ma (University of Massachusetts Amherst), Zhiqiang Lin (The Ohio State University)

BumbleBee: Secure Two-party Inference Framework for Large Transformers
Wen-jie Lu (Ant Group), Zhicong Huang (Ant Group), Zhen Gu (Alibaba Group), Jingyu Li (Ant Group & Zhejiang University), Jian Liu (Zhejiang University), Cheng Hong (Ant Group), Kui Ren (Zhejiang University), Tao Wei (Ant Group), WenGuang Chen (Ant Group)

Repurposing Neural Networks for Efficient Cryptographic Computation
Xin Jin (The Ohio State University), Shiqing Ma (University of Massachusetts Amherst), Zhiqiang Lin (The Ohio State University)

Session 4D: Blockchain Security 1 “Blockchain: Not Just for Cryptos”

Kronos: A Secure and Generic Sharding Blockchain Consensus with Optimized Overhead
Yizhong Liu (Beihang University), Andi Liu (Beihang University), Yuan Lu (Institute of Software Chinese Academy of Sciences), Zhuocheng Pan (Beihang University), Yinuo Li (Xi’an Jiaotong University), Jianwei Liu (Beihang University), Song Bian (Beihang University), Mauro Conti (University of Padua)

Manifoldchain: Maximizing Blockchain Throughput via Bandwidth-Clustered Sharding
Chunjiang Che (The Hong Kong University of Science and Technology (Guangzhou)), Songze Li (Southeast University), Xuechao Wang (The Hong Kong University of Science and Technology (Guangzhou))

Session 5B: Privacy & Anonymity "Mask On: Staying Anonymous in a World of Overexposure"

Session 5C: Federated Learning 1 "Learning Together, Securing Apart: The Federated Dilemma"

Session 5D: Side Channels 1 “Leaking Secrets: Side Channels That Don’t Have to Be Seen to Be Heard”

Session 6A: LLM Privacy and Usable Privacy “Large Language Models, Bigger Privacy Concerns”

I Know What You Asked: Prompt Leakage via KV-Cache Sharing in Multi-Tenant LLM Serving

Guanlong Wu (Southern University of Science and Technology), Zheng Zhang (ByteDance Inc.), Yao Zhang (ByteDance Inc.), Weili Wang (Southern University of Science and Technolog), Jianyu Niu (Southern University of Science and Technolog), Ye Wu (ByteDance Inc.), Yinqian Zhang (Southern University of Science and Technology (SUSTech))

IsolateGPT: An Execution Isolation Architecture for LLM-Based Agentic Systems

Yuhao Wu (Washington University in St. Louis), Franziska Roesner (University of Washington), Tadayoshi Kohno (University of Washington), Ning Zhang (Washington University in St. Louis), Umar Iqbal (Washington University in St. Louis)

Session 6B: Confidential Computing 1 “Shh! Keeping Secrets in the Cloud”

LeakLess: Selective Data Protection against Memory Leakage Attacks for Serverless Platforms

Maryam Rostamipoor (Stony Brook University), Seyedhamed Ghavamnia (University of Connecticut), Michalis Polychronakis (Stony Brook University)

Blindfold: Confidential Memory Management by Untrusted Operating System

Caihua Li (Yale University), Seung-seob Lee (Yale University), Lin Zhong (Yale University)

TME-Box: Scalable In-Process Isolation through Intel TME-MK Memory Encryption

Martin Unterguggenberger (Graz University of Technology), Lukas Lamster (Graz University of Technology), David Schrammel (Graz University of Technology), Martin Schwarzl (Cloudflare, Inc.), Stefan Mangard (Graz University of Technology)

Session 6C: Sensor Attacks “Your Sensors Are Watching...and They’re Vulnerable”

PhantomLiDAR: Cross-modality Signal Injection Attacks against LiDAR

Zizhi Jin (Zhejiang University), Qinhong Jiang (Zhejiang University), Xuancun Lu (Zhejiang University), Chen Yan (Zhejiang University), Xiaoyu Ji (Zhejiang University), Wenyuan Xu (Zhejiang University)

PowerRadio: Manipulate Sensor Measurement via Power GND Radiation

Yan Jiang (Zhejiang University), Xiaoyu Ji (Zhejiang University), Yancheng Jiang (Zhejiang University), Kai Wang (Zhejiang University), Chenren Xu (Peking University), Wenyuan Xu (Zhejiang University)

Interventional Root Cause Analysis of Failures in Multi-Sensor Fusion Perception Systems

Shuguang Wang (City University of Hong Kong), Qian Zhou (City University of Hong Kong), Kui Wu (University of Victoria), Jinghuai Deng (City University of Hong Kong), Dapeng Wu (City University of Hong Kong), Wei-Bin Lee (Information Security Center, Hon Hai Research Institute), Jianping Wang (City University of Hong Kong)

Session 6D: Software Security: Vulnerability Detection “Finding Bugs Before the Hackers Do”

Session 7A: Network Security 2 “Not Your Average Network: A Deep Dive into Security”

Session 7B: Trusted Hardware and Execution “The Trusted Hardware: No Secrets Left Inside”

Session 7C: Secure Protocols “Handshake With Caution: Securing the Digital Dialogue”

Session 7D: ML Security “Machine Learning...When Machines Learn to Hack You”

Session 8A: Email Security “Phishing for Trouble: Don’t Get Hooked”

Session 8B: Electromagnetic Attacks "Zap! The Shocking World of EMF Vulnerabilities"

Session 8C: Hard- & Firmware Security "The Bare Metal of Security: Protecting Hardware and Firmware"

Session 9B: DNN Attack Surfaces “Neural Networks Under Attack: When Deep Learning Gets Too Deep”

Session 9C: Phishing & Fraud 2 “Too Good to Be True: How Frauds Get the Hook”

Session 9D: Github + OSN Security “Code, Commit, and Commit to Security”

Woo Chung (S2W Inc.), Seungwon Shin (KAIST), Xiaojing Liao (Indiana University)

Rethinking Trust in Forge-Based Git Security

Aditya Sirish A Yelgundhalli (New York University), Patrick Zielinski (New York University), Reza Curtmola (New Jersey Institute of Technology), Justin Cappos (New York University)

Attributing Open-Source Contributions is Critical but Difficult: A Systematic Analysis of GitHub Practices and Their Impact on Software Supply Chain Security

Jan-Ulrich Holtgrave (CISPA Helmholtz Center for Information Security), Kay Friedrich (CISPA Helmholtz Center for Information Security), Fabian Fischer (CISPA Helmholtz Center for Information Security), Nicolas Huaman (Leibniz University Hannover), Niklas Busch (CISPA Helmholtz Center for Information Security), Jan H. Klemmer (CISPA Helmholtz Center for Information Security), Marcel Fourné (Paderborn University), Oliver Wiese (CISPA Helmholtz Center for Information Security), Dominik Wermke (North Carolina State University), Sascha Fahl (CISPA Helmholtz Center for Information Security)

Session 10A: Confidential Computing 2 “Sealed Envelopes: How Secure Is Your Data in the Box?”

WAVEN: WebAssembly Memory Virtualization for Enclaves

Weili Wang (Southern University of Science and Technology), Honghan Ji (ByteDance Inc.), Peixuan He (ByteDance Inc.), Yao Zhang (ByteDance Inc.), Ye Wu (ByteDance Inc.), Yinqian Zhang (Southern University of Science and Technology)

Secure Data Analytics in Apache Spark with Fine-grained Policy Enforcement and Isolated Execution

Byeongwook Kim (Seoul National University), Jaewon Hur (Seoul National University), Adil Ahmad (Arizona State University), Byoungyoung Lee (Seoul National University)

RContainer: A Secure Container Architecture through Extending ARM CCA Hardware Primitives

Qihang Zhou (Institute of Information Engineering, Chinese Academy of Sciences), Wenzhuo Cao (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyberspace Security, University of Chinese Academy of Sciences), Xiaoqi Jia (Institute of Information Engineering, Chinese Academy of Sciences), Peng Liu (The Pennsylvania State University, USA), Shengzhi Zhang (Department of Computer Science, Metropolitan College, Boston University, USA), Jiayun Chen (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyberspace Security, University of Chinese Academy of Sciences), Shaowen Xu (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyberspace Security, University of Chinese Academy of Sciences), Zhenyu Song (Institute of Information Engineering, Chinese Academy of Science)

Session 10B: Ransomware “When the Hacker’s Got the Key and You Don’t”

Session 10C: Privacy Preservation “How to Keep Secrets...Without Telling Anyone”

Session 10D: Machine Unlearning “Undoing the Machine's Memory: A Cyber Therapist’s Guide”

Provably Unlearnable Data Examples

Derui Wang (CSIRO's Data61), Minhui Xue (CSIRO's Data61), Bo Li (The University of Chicago), Seyit Camtepe (CSIRO's Data61), Liming Zhu (CSIRO's Data61)

Session 11A: Blockchain Security 2 “The Ledger of Lies: Securing the Blockchain Wild West”

Silence False Alarms: Identifying Anti-Reentrancy Patterns on Ethereum to Refine Smart Contract Reentrancy Detection

Qiyang Song (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences), Heqing Huang (Institute of Information Engineering, Chinese Academy of Sciences), Xiaoqi Jia (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences), Yuanbo Xie (Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences), Jiahao Cao (Institute for Network Sciences and Cyberspace, Tsinghua University)

PropertyGPT: LLM-driven Formal Verification of Smart Contracts through Retrieval-Augmented Property Generation

Ye Liu (Singapore Management University), Yue Xue (MetaTrust Labs), Daoyuan Wu (The Hong Kong University of Science and Technology), Yuqiang Sun (Nanyang Technological University), Yi Li (Nanyang Technological University), Miaolei Shi (MetaTrust Labs), Yang Liu (Nanyang Technological University)

Alba: The Dawn of Scalable Bridges for Blockchains

Giulia Scaffino (TU Wien), Lukas Aumayr (TU Wien), Mahsa Bastankhah (Princeton University), Zeta Avarikioti (TU Wien), Matteo Maffei (TU Wien)

Horcrux: Synthesize, Split, Shift and Stay Alive; Preventing Channel Depletion via Universal and Enhanced Multi-hop Payments

Anqi Tian (Institute of Software, Chinese Academy of Sciences; School of Computer Science and Technology, University of Chinese Academy of Sciences), Peifang Ni (Institute of Software, Chinese Academy of Sciences; Zhongguancun Laboratory, Beijing, P.R.China), Yingzi Gao (Institute of Software, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Jing Xu (Institute of Software, Chinese Academy of Sciences; University of Chinese Academy of Sciences；Zhongguancun Laboratory, Beijing, P.R.China)

Session 11B: Binary Analysis “Byte-Sized Mysteries: Decoding the Binary Jungle”

VeriBin: Adaptive Verification of Patches at the Binary Level

Hongwei Wu (Purdue University), Jianliang Wu (Simon Fraser University), Ruoyu Wu (Purdue University), Ayushi Sharma (Purdue University), Aravind Machiry (Purdue University), Antonio Bianchi (Purdue University)

Session 11C: Web Exploitation "The Web: It's Full of Exploits and You Don't Even Know"

Session 11D: Fuzzing 2 “More Fuzz, More Fun: Unleashing Chaos on Code”

Session 12A: Federated Learning 2 “Distributed Learning: Where Privacy Goes to Collaborate”

Session 12B: Malware "Malware: The Gift That Keeps on Giving (but in a Bad Way)"

Session 12C: Membership Inference “Who’s in the Club? Finding Out If You’re Targeted”

Black-box Membership Inference Attacks against Fine-tuned Diffusion Models
Yan Pang (University of Virginia), Tianhao Wang (University of Virginia)

Diffence: Fencing Membership Privacy With Diffusion Models
Yuefeng Peng (University of Massachusetts Amherst), Ali Naseh (University of Massachusetts Amherst), Amir Houmansadr (University of Massachusetts Amherst)

A Method to Facilitate Membership Inference Attacks in Deep Learning Models
Zitao Chen (University of British Columbia), Karthik Pattabiraman (University of British Columbia)

SIGuard: Guarding Secure Inference with Post Data Privacy
Xinqian Wang (RMIT University), Xiaoning Liu (RMIT University), Shangqi Lai (CSIRO Data61), Xun Yi (RMIT University), Xingliang Yuan (University of Melbourne)

Defending Against Membership Inference Attacks on Iteratively Pruned Deep Neural Networks
Jing Shang (Beijing Jiaotong University), Jian Wang (Beijing Jiaotong University), Kailun Wang (Beijing Jiaotong University), Jiqiang Liu (Beijing Jiaotong University), Nan Jiang (Beijing University of Technology), Md Armanuzzaman (Northeastern University), Ziming Zhao (Northeastern University)

Session 12D: ML Backdoors “Backdoors in ML: When the Algorithm Gets Tricked”

CLIBE: Detecting Dynamic Backdoors in Transformer-based NLP Models
Rui Zeng (Zhejiang University), Xi Chen (Zhejiang University), Yuwen Pu (Zhejiang University), Xuhong Zhang (Zhejiang University), Tianyu Du (Zhejiang University), Shouling Ji (Zhejiang University)

Try to Poison My Deep Learning Data? Nowhere to Hide Your Trajectory Spectrum!
Yansong Gao (The University of Western Australia), Huaibing Peng (Nanjing University of Science and Technology), Hua Ma (CSIRO's Data61), Zhi Zhang (The University of Western Australia), Shuo Wang (Shanghai Jiao Tong University), Rayne Holland (CSIRO's Data61), Anmin Fu (Nanjing University of Science and Technology), Minhui Xue (CSIRO's Data61), Derek Abbott (The University of Adelaide, Australia)

LADDER: Multi-Objective Backdoor Attack via Evolutionary Algorithm
Dazhuang Liu (Delft University of Technology), Yanqi Qiao (Delft University of Technology), Rui Wang (Delft University of Technology), Kaitai Liang (Delft University of Technology), Georgios Smaragdakis (Delft University of Technology)

Session 13A: JavaScript Security “Script Kiddies Beware: Securing the Web’s Wild West”

Session 13B: API Security “Behind the Curtain: Securing the Magic of APIs”

Session 13C: Side Channels 2 “More Than You Bargained for: The Sneaky Side Channels”

Session 13D: Software Security: Code and Compiler “Compiling a Plan to Secure Your Code”

Session 14A: Software Security: Applications & Policies “Apps, Rules, and the Never-Ending Game of Security”

Session 14B: Privacy & Cryptography 2 “Crypto’s Secret: Keeping It Safe, Keeping It Quiet”

East China Normal University), Zhenfu Cao (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University), Guomin Yang (School of Computing and Information Systems, Singapore Management University), Robert H. Deng (School of Computing and Information Systems, Singapore Management University)

Session 14C: Vulnerability Detection “Vulnerability Hunting: The Quest for the Perfect Patch”

Be Careful of What You Embed: Demystifying OLE Vulnerabilities

Yunpeng Tian (Huazhong University of Science and Technology), Feng Dong (Huazhong University of Science and Technology), Haoyi Liu (Huazhong University of Science and Technology), Meng Xu (University of Waterloo), Zhiniang Peng (Huazhong University of Science and Technology; Sangfor Technologies Inc.), Zesen Ye (Sangfor Technologies Inc.), Shenghui Li (Huazhong University of Science and Technology), Xiapu Luo (The Hong Kong Polytechnic University), Haoyu Wang (Huazhong University of Science and Technology)

From Large to Mammoth: A Comparative Evaluation of Large Language Models in Vulnerability Detection

Jie Lin (University of Central Florida), David Mohaisen (University of Central Florida)

Sheep's Clothing, Wolf's Data: Detecting Server-Induced Client Vulnerabilities in Windows Remote IPC

Fangming Gu (Institute of Information Engineering, Chinese Academy of Sciences), Qingli Guo (Institute of Information Engineering, Chinese Academy of Sciences), Jie Lu (Institute of Computing Technology, Chinese Academy of Sciences), Qinghe Xie (Institute of Information Engineering, Chinese Academy of Sciences), Beibei Zhao (Institute of Information Engineering, Chinese Academy of Sciences), Kangjie Lu (University of Minnesota), Hong Li (Institute of information engineering, Chinese Academy of Sciences), Xiaorui Gong (Institute of information engineering, Chinese Academy of Sciences)

Session 14D: Autonomous Vehicles “Hacking the Wheel: When Self-Driving Cars Get ‘Lost’”

On the Realism of LiDAR Spoofing Attacks against Autonomous Driving Vehicle at High Speed and Long Distance

Takami Sato (University of California, Irvine), Ryo Suzuki (Keio University), Yuki Hayakawa (Keio University), Kazuma Ikeda (Keio University), Ozora Sako (Keio University), Rokuto Nagata (Keio University), Ryo Yoshida (Keio University), Qi Alfred Chen (University of California, Irvine), Kentaro Yoshioka (Keio University)

Revisiting Physical-World Adversarial Attack on Traffic Sign Recognition: A Commercial Systems Perspective

Ningfei Wang (University of California, Irvine), Shaoyuan Xie (University of California, Irvine), Takami Sato (University of California, Irvine), Yunpeng Luo

Message from the General Chairs

Welcome to the 2025 Network and Distributed System Security (NDSS) Symposium!

This year, the organizing and technical program committees have put together an exceptional program featuring 211 papers, two distinguished keynotes—Johanna Sepúlveda, Senior Expert and Technical Domain Manager for Quantum and Quantum-Secure Technologies at Airbus Defence and Space, and Kathleen Fisher, Director of DARPA/I2O—along with a poster session showcasing 37 posters and eight co-hosted events.

A program of this scale would not be possible without the dedication of numerous volunteers, and we extend our deepest gratitude to them.

First, we thank our Technical Program Committee Co-Chairs, Christina Pöpper and Hamed Okhravi, for curating an outstanding technical program. NDSS 2025 had two submission cycles, and we appreciate the program committee members and external reviewers for their meticulous work in reviewing submissions, guiding authors through revisions, and selecting the best papers for presentation.

Second, we are grateful to Daniele Cono D'Elia and Mathy Vanhoef for leading the artifact evaluation initiative, which evaluated 63 artifacts. We also extend a huge thanks to Mridula Singh and Hyungsub Kim, our publications chairs, for ensuring the collection and timely publication of camera-ready papers.

Additionally, we appreciate Jelena Mirkovic and Sébastien Bardin for organizing an impressive set of co-located events this year, including:

1. Security and Privacy of Next-Generation Networks (FutureG)
2. Security and Privacy in Standardized IoT (SDIoTSec)
3. Security of Space and Satellite Systems (SpaceSec)
4. Usable Security and Privacy (USEC)
5. SOC Operations and Construction (WOSOC)
6. Binary Analysis Research (BAR)
7. Innovation in Metadata Privacy: Analysis and Construction Techniques (IMPACT)
8. Measurements, Attacks, and Defenses for the Web (MADWeb)

We also extend our thanks to Tianshi Li and Kaushal Kafle for coordinating a fantastic poster session, and for organizing the Best Poster Awards. Special appreciation goes to Tingting Chen and her team for reviewing student fellowship applications—this year, 31 students received NDSS fellowships and travel support.

Further thanks to Yue Xiao, our publicity chair, and Tom Hutton, our local arrangements chair. We also acknowledge the NDSS Steering Group led by Yongdae Kim for their guidance and active participation in making this symposium a success.

Acknowledging Our Sponsors

NDSS is made possible through the generous support of our sponsors. We extend our gratitude to:

> Gold Sponsor TikTok; Coffee Break Sponsor Google; Silver Sponsors Ant Group, Amazon Science, FutureWei Technologies, and Palo Alto Networks; and our lanyard sponsor Qualcomm. Palo Alto Networks also sponsored a Best Paper award for the MADWeb workshop.

We also thank our sponsorship coordinators—Yongdae Kim, Heng Yin, and Mauro Conti—for their efforts in helping identify potential sponsors around the globe.

Thank You to ISOC & AMS

NDSS would not happen without the invaluable support of the ISOC team—Raquel Kroich, Sally Harvey, Robin Wilton, Robbie Mitchell, and Ivana Trbovic. We sincerely appreciate the Internet Society's continued support of NDSS, as well as the Association Management Solutions (AMS) staff for their ongoing efforts in managing this event.

And Finally, Thank You!

Most importantly, thank you to all of you—our participants! NDSS exists because of your contributions. Whether you are submitting and presenting papers and posters, attending sessions, or engaging in discussions, your participation strengthens our community in network and distributed system security.

We hope you enjoy NDSS 2025!

David Balenson and Heng Yin
General Chairs, NDSS 2025

Message from the Program Committee Co-Chairs

We are delighted to present the technical program of the 2025 Network and Distributed System Security (NDSS) symposium, held as an in-person event between February 24 and 28, 2025. Now in its 33rd edition and hosted by the Internet Society (ISOC) from the start, NDSS has established itself as a top-tier academic conference focused on cybersecurity research, particularly in network and system security. NDSS emphasizes practical and impactful security solutions for research and practice, making it highly relevant to both academia and industry.

The field of cybersecurity is experiencing rapid growth and transformation. This year, a total of 1311 submissions entered the peer review process over two submission cycles (this does not count papers that clearly violated the submission guidelines or were judged as out of scope by a PC subcommittee). The submissions were evaluated on the basis of their technical quality, novelty, and significance. Two rounds of reviewing (and in some cases additional reviews) in each cycle and additional assessments by the newly established Ethics Review Board (if applicable) were conducted. Papers with two clearly negative reviews were early rejected after the first round, the others advanced to the second round for another set of reviews. More than 83% of the 544 papers entering the second review round received a total of four reviews (or more), the others three reviews. We strove to make the review process competitive but constructive and insightful for the authors, including a rebuttal and interactive discussion phase. Program Committee (PC) members were regularly reminded to identify positive points in the submission and provide concrete suggestions to improve each paper; 103 papers were accepted after major revisions. At the end of the review process and after intense online discussions, 211 papers (16.1% acceptance rate) were selected to appear in the program. 68 of the accepted papers additionally submitted their artifacts for review of the Artifact Evaluation committee, 63 of which were evaluated in their entirety. Navigating the use of Generative AI and enforcing integrity and review ethics throughout the review process were two aspects where we devoted particular attention.

We would like to extend our sincere thanks to the PC members and external reviewers. The task of the PC members was substantial as we asked them to contribute significant time and effort in the expert selection of papers. 167 experts accepted our invitation to join the NDSS ’25 Technical Program Committee, 119 of whom participated in both review cycles. The PC members wrote up to 10 reviews in the Summer Cycle and up to 18 reviews in the Fall cycle. In addition, they participated in the online PC discussion, in the interactive discussion phase with the authors, and many served as shepherds for minor revisions or discussion leads for major revisions (where the revisions were reassessed by all reviewers). We would like to express our sincere gratitude to them - without their service NDSS would not be possible. We also extend our thanks to the members of the Artifact Evaluation Committee who each assessed three or more artifacts.

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 name a few individuals who made particular contributions to NDSS 2025. David Balenson served as Chair of the Organization Committee and was an invaluable source of information and institutional knowledge, guiding us with his expertise. Steering Committee Chair Yongdae Kim provided strategic oversight and worked closely with us on key decisions and navigating complex cases where additional insight was needed—our sincere thanks to him and the entire Steering Committee. Robin Wilton played a pivotal role as a bridge between the Program Co-Chairs, the Organizing Committee, and ISOC and was crucial to ensuring that every moving part stayed in sync—all while infusing the process with enthusiasm. From ISOC, Joseph Hall offered valuable support, and Ivana Trbovic did an excellent job regarding website management. Artifact Evaluation Co-Chairs Daniele Cono D'Elia and Mathy Vanhoef ran the artifact evaluation process with exceptional diligence, reinforcing its role as a cornerstone of rigorous research and marking the second time NDSS has embraced this initiative. Mridula Singh and Hyungsub Kim expertly managed the intricate details of proceedings production. It has been an honor to work with all of you!

Finally, we thank all authors who submitted to NDSS 2025 and all attendees who are joining us in person—without you, NDSS would not be possible. We also thank the selected presenters joining us online; we are sorry you could not make it in person for reasons beyond your control.

We hope you will enjoy the new location in San Diego and are accepting a few possible relocation hiccups. Enjoy the conference!

Christina Pöpper and Hamed Okhravi
Program Committee Co-Chairs, NDSS 2025

Message from the Internet Society

The Internet Society is once again proud to host the Network and Distributed System Security (NDSS) Symposium in 2025, continuing our decades-long commitment to NDSS. The Symposium remains in the top four global security conferences, which is a testament to the impact of your research 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. Our work is enabled and supported by the research you carry out, the leaders you develop, and the breakthroughs you achieve. Through your efforts and NDSS' open publication policy, the state of the art in network and distributed systems security is advanced, world wide. Thank you.

In 2025, NDSS continues to set new records. Paper submissions doubled (again!), from 700 to 1372, and by expanding NDSS from three tracks to four, for the first time, we have been able to accommodate 211 accepted papers: an increase of one third over 2024. With an acceptance rate of just over 15%, that meant competition to present papers at NDSS 2025 was extremely tough: congratulations to the successful teams.

Those record numbers have, of course, meant a sharp increase in workload for the huge number of volunteers from the community who put together this high-quality program. The Program Committee alone, this year, consisted of almost 170 volunteers, peer reviewing and scoring the record number of submissions.

We are grateful for the hard work undertaken by General Co-Chairs David Balenson and Heng Yin, Program Committee Co-Chairs Christina Pöpper and Hamed Okhravi, and the Organizing and Program Committee members who have invested countless hours to review papers and posters, evaluate research artifacts, publish the proceedings, organize co-located sessions, and improve the NDSS student support program.

As ever, the Program Committee has lined up two world-class keynote speakers, in Dr Johanna Sepúlveda (Airbus Defence and Space) and Dr Kathleen Fisher (DARPA), who will share their insights on cutting-edge technologies in a turbulent geo-political environment.

Finally, I am profoundly grateful to the sponsors without whom this event would not be possible. This includes our Gold Sponsor TikTok; Coffee Break Sponsor Google; Silver Sponsors Ant Group, Amazon Science, FutureWei Technologies, and Palo Alto Networks; and our lanyard sponsor Qualcomm. Palo Alto Networks have also sponsored a Best Paper award for the MADWeb workshop.

On behalf of the Internet Society, I welcome you to the busiest ever NDSS. The opportunities to learn, network, and develop are almost limitless: I hope you find time to have some fun too!

Sally Wentworth
President and CEO, Internet Society

Program Committee

Christina Pöpper, *New York University Abu Dhabi* (Co-Chair)
Hamed Okhravi, *MIT Lincoln Laboratory* (Co-Chair)

Abhishta Abhishta, *University of Twente*
Adam Bates, *University of Illinois at Urbana-Champaign*
Adwait Nadkarni, *William & Mary*
Ahmad-Reza Sadeghi, *TU Darmstadt*
Alessandro Sorniotti, *IBM Research Europe*
Alexandra Dmitrienko, *University of Wuerzburg*
Ali Abbasi, *CISPA Helmholtz Center for Information Security*
Alvaro Cardenas, *University of California, Santa Cruz*
Amy Babay, *University of Pittsburgh*
Ang Li, *The University of Michigan-Dearborn*
Angelos Stavrou, *Virginia Tech*
Antonio Villani, *Retooling*
Aolin Ding, *Accenture Labs*
Aravind Machiry, *Purdue University*
Awais Rashid, *University of Bristol*
Bahruz Jabiyev, *Dartmouth College*
Bart Coppens, *Ghent University*
Ben Stock, *CISPA Helmholtz Center for Information Security*
Benjamin Ujcich, *Georgetown University*
Benjamin Andow, *Google*
Binbin Zhao, *Georgia Institute of Technology*
Brendan Saltaformaggio, *Georgia Institute of Technology*
Christine Utz, *Radboud University*
Christof Ferreira Torres, *ETH Zurich*
Christophe Hauser, *Dartmouth College*
Christopher Kruegel, *UC Santa Barbara*
Claudio Soriente, *NEC Laboratories Europe*
Coby Wang, *Visa Research*
Daniel Gruss, *Graz University of Technology*
Daniele Cono D'Elia, *Sapienza University of Rome*
Daoyuan Wu, *Hong Kong University of Science and Technology*
David Mohaisen, *University of Central Florida*
Derrick McKee, *MIT Lincoln Laboratory*
Derui Wang, *CSIRO's Data61*
Ding Wang, *Nankai University*
Doowon Kim, *University of Tennessee, Knoxville*
Eleonora Losiouk, *University of Padua*
Erik van der Kouwe Vrije, *Universiteit Amsterdam*
Faysal Hossain Shezan, *University of Texas at Arlington*

Fengwei Zhang, *Southern University of Science and Technology*
Flavio Toffalini, *EPFL*
Gang Qu, *University of Maryland*
Gary Tan, *Pennsylvania State University*
Ghassan Karame, *Ruhr University Bochum*
Giovanni Apruzzese, *University of Liechtenstein*
Guangdong Bai, *The University of Queensland*
Guofei Gu, *Texas A&M University*
Habiba Farrukh, *University of California, Irvine*
Haibin Zhang, *Yangtze Delta Region Institute of Tsinghua University*
Haipeng Cai, *Washington State University*
Han Qiu, *Tsinghua University*
Haojin Zhu, *Shanghai Jiao Tong University*
Hong Hu, *Pennsylvania State University*
Hongxin Hu, *University at Buffalo*
Hossein Fereidooni, *KOBIL GmbH*
Houman Homayoun, *University of California Davis*
Hyungsub Kim, *Indiana University*
Imtiaz Karim, *Purdue University*
Insu Yun, *KAIST*
Ivan Martinovic, *University of Oxford*
Jason (Minhui) Xue, *CSIRO's Data61*
Jianjun Chen, *Tsinghua University*
Juan Tapiador, *Carlos III University of Madrid*
Jun Xu, *University of Utah*
Juraj Somorovsky, *Paderborn University*
JV Rajendran, *Texas A&M University*
Kai Li, *San Diego State University*
Kaihua Qin, *Yale University*
Kaushal Kafle, *University of South Florida*
Kevin Borgolte, *Ruhr University Bochum*
Kevin Leach, *Vanderbilt University*
Kun Sun, *George Mason University*
Kyungtae Kim, *Dartmouth College*
Lannan Lisa Luo, *George Mason University*
Le Guan, *University of Georgia*
Lejla Batina, *Radboud University*
Lingyu Wang, *Concordia University*
Lorenzo Cavallaro, *University College London*
Manuel Egele, *Boston University*
Marcus Botacin, *Texas A&M University*
Marcus Peinado, *Microsoft Research*
Marko Vukolic, *ConsensusLab*

Martin Strohmeier, *Cyber-Defence Campus, armasuisse Science + Technology*
Martin Henze, *RWTH Aachen University & Fraunhofer FKIE*
Martin Johns, *TU Braunschweig*
Mathias Payer, *EPFL*
Matteo Grosse-Kampmann, *Rhine-Waal University / AWARE7 GmbH*
Meng Luo, *Zhejiang University*
Meng Xu, *University of Waterloo*
Michael Schwarz, *CISPA Helmholtz Center for Information Security*
Mihalis Maniatakos, *NYU Abu Dhabi*
Min Suk Kang, *KAIST*
Ming Li, *The University of Texas at Arlington*
Minghong Fang, *Duke University*
Mingxue Zhang, *Zhejiang University*
Mitsuaki Akiyama, *NTT*
Mohammad Islam, *University of Texas at Arlington*
Mu Zhang, *University of Utah*
Murtuza Jadliwala, *University of Texas at San Antonio*
Nader Sehatbakhsh, *UCLA*
Nadim Kobeissi, *Cure53, Symbolic Software*
Nathan Burow, *MIT Lincoln Laboratory*
Neil Gong, *Duke University*
Nick Nikiforakis, *Stony Brook University*
Nidhi Rastogi, *Rochester Institute of Technology*
Ning Wang, *University of South Florida*
Omar Chowdhury, *Stony Brook University*
Paria Shirani, *University of Ottawa*
Peng Gao, *Virginia Tech*
Per Larsen, *Immunant, Inc.*
Phani Vadrevu, *Louisiana State University*
Prashast Srivastava, *Columbia University*
Qi Li, *Tsinghua University*
Qiang Tang, *The University of Sydney*
Qiben Yan, *Michigan State University*
Qingchuan Zhao, *City University of Hong Kong*
Qiushi Wu, *IBM Research*
Rachel Greenstadt, *New York University*
Raghavendran Ramakrishnan, *Snowflake Inc*
Rajvardhan Oak, *University of California Davis / Microsoft Corporation*
René Mayrhofer, *Johannes Kepler University Linz*
Rob Cunningham, *University of Pittsburgh*
Ruoyu “Fish” Wang, *Arizona State University*
Saman Zonouz, *Georgia Institute of Technology*
Samuel Jero, *MIT Lincoln Laboratory*

Sandra Siby, *Imperial College London*
Sang Kil Cha, *KAIST*
Santosh Nagarakatte, *Rutgers University*
Sebastian Köhler, *University of Oxford*
Sébastien Bardin, *CEA List, Université Paris Saclay*
Shagufta Mehnaz, *Pennsylvania State University*
Shahin Tajik, *Worcester Polytechnic Institute*
Sherman S. M. Chow, *Chinese University of Hong Kong*
Shweta Shinde, *ETH Zurich*
Sisi Duan, *Tsinghua University*
Soheil Salehi, *The University of Arizona*
Srdjan Čapkun, *ETH Zurich*
Stephen Herwig, *William & Mary*
Stjepan Picek, *Radboud University*
Suryadipta Majumdar, *Concordia University*
Syed Rafiul Hussain, *Pennsylvania State University*
Takuya Watanabe, *Deloitte Tohmatsu Cyber LLC*
Tatsuya Mori, *Waseda University*
Theodor Schnitzler, *Maastricht University*
Tianhao Wang, *University of Virginia*
Ting Wang, *Stony Brook University*
Tuba Yavuz, *University of Florida*
Veelasha Moonsamy, *Ruhr University Bochum*
Wajih Ul Hassan, *University of Virginia*
Wenke Lee, *Georgia Institute of Technology*
William Robertson, *Northeastern University*
Xiaokuan Zhang, *George Mason University*
Xingliang Yuan, *The University of Melbourne*
Xinwen Fu, *University of Massachusetts Lowell*
Xinyang Ge, *Databricks*
Xinyu Xing, *Northwestern University*
Yang Zhang, *CISPA Helmholtz Center for Information Security*
Yongdae Kim, *KAIST*
Yonghwi Kwon, *University of Maryland*
Yuan Hong, *University of Connecticut*
Yue Zhang, *Drexel University*
Yuzhe Tang, *Syracuse University*
Z. Berkay Celik, *Purdue University*
Zephyr Yao, *New Jersey Institute of Technology*
Zhikun Zhang, *Stanford & CISPA*
Zhiyun Qian, *University of California, Riverside*
Zhou Li, *University of California, Irvine*

External Reviewers

Aashutosh Poudel, *William & Mary*
Abdullah Al Ishtiaq, *Pennsylvania State University*
Alan Liu, *University of Maryland*
Alexander Herzog, *University College London*
Aliai Eusebi, *University College London*
Alireza Moghaddas Borhan, *Concordia University*
Amit Seal Ami, *William & Mary*
Ananth Shreekumar, *Purdue University*
Andes Y. L. Kei, *The Chinese University of Hong Kong*
Andreas Kogler, *Graz University of Technology*
Andrei Homescu, *Immunant, Inc.*
Arash Daneshmand, *Concordia University*
Atri Bhattacharyya, *Oracle*
Azadeh Tabiban, *University of Manitoba*
Baohang Huang, *Beijing Institute of Technology*
Beomseok Oh, *KAIST*
Burak Sahin, *Georgia Institute of Technology*
Chathura Rajapaksha, *Boston University*
Chen Gong, *University of Virginia*
Chengkai Weng, *Arizona State University*
CheolJun Park, *Kyung Hee University*
Christoforos Vasilatos, *New York University Abu Dhabi*
Congyu Liu, *Purdue University*
Daniel Klischies, *Ruhr University Bochum*
Danyu Sun, *University of California, Irvine*
Dohyun Kim, *KAIST*
Duckwoo Kim, *KAIST*
Dunia Mahboobeh, *New York University Abu Dhabi*
Eduardo Chielle, *New York University Abu Dhabi*
Elisa Braconaro, *Università degli Studi di Padova*
Emily Shen, *MIT Lincoln Laboratory*
Eric Wagner, *Fraunhofer FKIE & RWTH Aachen University*
Fabian Rauscher, *Graz University of Technology*
Felix Lange, *Paderborn University*
Florian Hantke, *CISPA*
Gianluca Capozzi, *Università Roma “La Sapienza”* and *University College London*
Hamid Bostani, *Radboud University*
Han Zheng, *EPFL*
Hannes Weissteiner, *Graz University of Technology*
Hansung Bae, *KAIST*
Haochen Wang, *Tsinghua University*
Haoran Yang, *Washington State University*

Harry W. H. Wong, *The Chinese University of Hong Kong*
Hengkai Ye, *Pennsylvania State University*
Hinddeep Purohit, *Concordia University*
Hithem Lamri, *New York University Abu Dhabi*
Homer Gamil, *New York University Abu Dhabi*
Huancheng Zhou, *Texas A&M University*
Hugo Kermabon-Bobinnec, *Concordia University*
Hyeonmin Lee, *University of Virginia*
Hyunmin Ju, *KAIST*
Ioannis Angelakopoulos, *Boston University*
Jack P. K. Ma, *The Chinese University of Hong Kong*
Jaehoon Kim, *KAIST*
Jan Horacek, *Johannes Kepler University Linz*
Jan Pennekamp, *RWTH Aachen University*
Jannis Rautenstrauch, *CISPA*
Jiacen Xu, *University of California, Irvine*
Jiafan Wang, *CSIRO's Data61*
Jianwei Huang, *Texas A&M University*
Jiawei Guo, *University at Buffalo*
Jing Xu, *Chinese Academy of Sciences*
Joann Chen, *University of California, Irvine*
Jonas Juffinger, *Graz University of Technology*
Jose Miguel Moreno, *University Carlos III of Madrid*
Ju Chen, *Meta*
Juanita Gomez, *University of California, Santa Cruz*
Juliana Furgala, *MIT Lincoln Laboratory*
Jung Hyun Kim, *KAIST*
Jungwoo Lee, *KAIST*
Kai Tu, *Pennsylvania State University*
Kailun Yan, *George Mason University*
Keerthi Koneru, *University of California, Santa Cruz*
Keika Mori, *Deloitte Tohmatsu Cyber LLC*
Keyan Guo, *University at Buffalo*
Konrad Wolsing, *Fraunhofer FKIE & RWTH Aachen University*
Kwangmin Kim, *KAIST*
Lucien K. L. Ng, *Georgia Institute of Technology*
Luis Burbano, *University of California, Santa Cruz*
Lukas Giner, *Graz University of Technology*
Manaar Alam, *New York University Abu Dhabi*
Manki Cho, *KAIST*
Mario Lins, *Johannes Kepler University Linz*
Maximilian Radoy, *Paderborn University*
Mengxiao Wang, *Texas A&M University*
Michael Roland, *Johannes Kepler University Linz*

Mincheol Son, *KAIST*
Mingfei Zhang, *Shandong University*
Minxin Du, *Hong Kong Polytechnic University*
Mohammed Nabeel, *New York University Abu Dhabi*
Mujtahid Al Akon, *Pennsylvania State University*
Nicholas Miazzo, *Università degli Studi di Padova*
Nico Heitmann, *Paderborn University*
Niklas Niere, *Paderborn University*
Pankaj Niroula, *William & Mary*
Peiyang Li, *Tsinghua University*
Philipp Mackensen, *Ruhr University Bochum*
Prianka Mandal, *William & Mary*
Qifan Zhang, *University of California, Irvine*
Qiqing Huang, *University at Buffalo*
Raymond Muller, *Purdue University*
Ritik Roongta, *New York University*
Roland Czerny, *Graz University of Technology*
Ruixuan Liu, *Emory University*
Rujia Li, *Tsinghua University*
Ruoyu Song, *Purdue University*
Rupam Patir, *University at Buffalo*
Saleh Khalaj Monfared, *Worcester Polytechnic Institute*
Samuele Doria, *Università degli Studi di Padova*
Sangmin Woo, *KAIST*
Sangwook Bae, *Cape*
Sareh Mohammadi, *Concordia University*
Sebastian Castro, *University of California, Santa Cruz*
Seyed Mohammadjavad Seyed Talebi, *Pyte*
Shreyas Kumar, *Texas A&M University*
Shuangpeng Bai, *Pennsylvania State University*
Shubham Agarwal, *CISPA*
Shujaat Mirza, *ML Alignment & Theory Scholars (MATS)*
Siji Chen, *Tsinghua University*
Song Liu, *Pennsylvania State University*
Soomin Kim, *KAIST*
Stefan Gast, *Graz University of Technology*
Stefan Saroiu, *Microsoft Research*
Sven Hebrok, *Paderborn University*
Syed Md Mukit Rashid, *Pennsylvania State University*
Taekkyung Oh, *KAIST*
Tianchang Yang, *Pennsylvania State University*
Tianwei Wu, *Pennsylvania State University*
Tobias Höller, *Johannes Kepler University Linz*
Tuan Dinh Hoang, *KAIST*

Vamsi Simhadri, *George Mason University*
Victor Olaiya, *William & Mary*
Vishnu Teja Kandalam, *George Mason University*
Wanda Guo, *Texas A&M University*
Wanlun Ma, *Swinburne University of Technology*
Wei Zhou, *Huazhong University of Science and Technology*
Wen Li, *Utah State University*
Xiao Sui, *Tsinghua University*
Xiaochen Li, *University of Virginia*
Xiaoyun Xu, *Radboud University*
Xin Wang, *Tsinghua University*
Xingzhi Qian, *University College London*
Xinhao Deng, *Tsinghua University*
Xinran Zheng, *University College London*
Xuanji Meng, *Tsinghua University*
Xuesong Bai, *University of California, Irvine*
Yan Pang, *University of Virginia*
Yichang Xiong, *George Mason University*
Yihao Chen, *Tsinghua University*
Yilu Dong, *Pennsylvania State University*
Yixin Sun, *University of Virginia*
Youwei Shu, *National University of Singapore*
Yu Liang, *Pennsylvania State University*
Yu Nong, *University at Buffalo*
Yu Zheng, *University of California, Irvine*
Yu Zheng, *University of California, Irvine*
Yucheng Fu, *University of Virginia*
Yuji Sakurai, *Deloitte Tohmatsu Cyber LLC*
Yunpeng Liu, *Tsinghua University*
Yuqi Qing, *Tsinghua University*
Yuxin Cao, *National University of Singapore*
Zhaoyang Xie, *Beijing Institute of Technology*
Zhechang Zhang, *Pennsylvania State University*
Zhengyuan Jiang, *University of South Florida*
Zhiyong Fang, *Texas A&M University*
Zihang Xiang, *KAUST*

Artifact Evaluation Committee

Advije Rizvani, *University of Liechtenstein*
Ahmed Lekssays, *Qatar Computing Research Institute*
Alessandro Erba, *Karlsruhe Institute of Technology*
Amit Samanta, *University of Utah*
Andrew Roberts, *Tallinn University of Technology*
Aolin Ding, *Accenture Labs*
Ayomide Akinsanya, *Stevens Institute of Technology*
Cen Zhang, *Nanyang Technological University*
CheolJun Park, *Kyung Hee University*
Christoph Sendner, *University of Würzburg*
Cristian Assaiante, *Sapienza University of Rome*
Dipsy Desai, *University of Southern California*
Dongwei Xiao, *The Hong Kong University of Science and Technology*
Evangelos Bitsikas, *Northeastern University*
Felix Lange, *Paderborn University*
Fuman Xie, *The University of Queensland*
Gertjan Franken, *DistriNet at KU Leuven*
Guangjing Wang, *University of South Florida*
Hao Cui, *University of California, Irvine*
Héloïse Gollier, *DistriNet at KU Leuven*
Hengkai Ye, *Penn State University*
Hongyan Chang, *National University of Singapore*
Jan Jancar, *Masaryk University*
Jeroen Robben, *DistriNet at KU Leuven*
Jessy Ayala, *University of California, Irvine*
Jiahao Yu, *Northwestern University*
Jing Liu, *UC Irvine & MPI-SP*
Kelly Kaoudis, *Trail of Bits*
Marc Damie, *University of Twente/Inria*
Marton Bognar, *DistriNet at KU Leuven*
Matteo Marini, *Sapienza University of Rome*
Mir Masood Ali, *University of Illinois Chicago*
Nico Heitmann, *Paderborn University*
Naman Gupta, *University of Wisconsin-Madison*
Niklas Niere, *Paderborn University*
Paul Staat, *Max Planck Institute for Security and Privacy*
Pedro Bernardo, *TU Wien*
Prajwal Panzade, *Old Dominion University*
Qifan Zhang, *University of California, Irvine*
Rajrup Ghosh, *University of Southern California*
Rishit Saiya, *PwC*

Ryan Vrecenar, *Sandia National Laboratories*
Salvatore Signorello, *Telefonica Research Spain*
Shaofeng Li, *Peng Cheng Laboratory*
Shenghan Zheng, *UC Riverside*
Steven Ngo, *University of California, Irvine*
Tillson Galloway, *Georgia Institute of Technology*
Tolga Atalay, *Virginia Tech*
Torsten Krauß, *University of Würzburg*
Tristan Benoit, *Universität der Bundeswehr München*
Vik Vanderlinden, *DistriNet at KU Leuven*
Vinny Adjibi, *Georgia Institute of Technology*
Xu He, *George Mason University*
Xuan Xie, *University of Alberta*
Xuesong Bai, *University of California, Irvine*
Yi Liu, City *University of Hong Kong*
Yiming Zhang, *Tsinghua University*
Yirui He, *University of California, Irvine*
Yu Nong, *Washington State University*
Yujin Huang, *The University of Melbourne*
Zheng Yu, *Northwestern University*
Zhengxiong Luo, *National University of Singapore*
Zilong Lin, *Indiana University Bloomington*

Ethical Review Board (ERB) Members

Srdjan Čapkun, *ETH Zurich (Chair)*
Aravind Machiry, *Purdue University*
Juan Tapiador, *Carlos III University of Madrid*
Rachel Greenstadt, *New York University*
René Mayrhofer, *Johannes Kepler University Linz*
William Robertson, *Northeastern University*

Organizing Committee

General Chairs

David Balenson
USC Information Sciences Institute

Heng Yin
University of California, Riverside

Program Committee Co-Chairs

Christina Pöpper
NYU Abu Dhabi

Hamed Okhravi
MIT Lincoln Laboratory

Artifact Evaluation Committee Co-Chairs

Daniele Cono D'Elia
Sapienza University

Mathy Vanhoef
KU Leuven

Workshop Co-Chairs

Jelena Mirkovic
USC Information Sciences Institute

Sébastien Bardin
CEA LIst

Poster Session Co-Chairs

Tianshi Li
Northeastern University

Kaushal Kafle
University of South Florida

Publicity Chair

Yue Xiao
Indiana University Bloomington

Publications Co-Chairs

Mridula Singh
CISPA

Hyungsub Kim
Indiana University Bloomington

Local Arrangements Chair

Tom Hutton
San Diego Supercomputer Center

Sponsorship Coordinators

Yongdae Kim
KAIST

Heng Yin
University of California, Riverside

Mauro Conti
University of Padua

The Internet Society/Foundation Staff

Raquel Kroich
Event Manager

Robin Wilton
Program Liaison

Ivana Trbovic
Website Manager

Sally Harvey
Sponsorships

Robbie Mitchell
Publicity

Student Support Committee

Tingting Chen (Chair)
Cal Poly Pomona

Younghee Park
San Jose State University

Lei Yu
Rensselaer Polytechnic Institute

Eric Chan-Tin
Loyola University Chicago

Huirong Fu
Oakland University

Steering Group

Co-Chairs

Yongdae Kim
KAIST

Robin Wilton
Internet Society

Steering Group Members

Christopher Kruegel
UC Santa Barbara

Wenyuan Xu
Zhejiang University

Gabriela Ciocarlie
University of Texas at San Antonio

Daphne Yao
Virginia Tech

Ahmad-Reza Sadeghi
TU Darmstadt

Michael Reiter
Duke University

Gene Tsudik
UC Irvine

Lorenzo Cavallaro
University College London

Anita Nikolich
UIUC