Proceedings

2026

Network and Distributed System Security Symposium

Proceedings

2026

Network and Distributed System Security Symposium

February 23 – February 27, 2026

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.

ISBN Number (Digital Format): 979-8-9919276-8-0

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
Artifact Evaluation Committee
Ethical Review Board (ERB) Members
Organizing Committee
Steering Group

Session 1A: Session 1A: Network Security The Fast and the Curious Packets

A Hard-Label Black-Box Evasion Attack against ML-based Malicious Traffic Detection Systems
Zixuan Liu (Tsinghua University), Yi Zhao (Beijing Institute of Technology), Zhuotao Liu (Tsinghua University and Zhongguancun Lab), Qi Li (Tsinghua University and Zhongguancun Lab), Chuanpu Fu (Tsinghua University), Guangmeng Zhou (Tsinghua University), Ke Xu (Tsinghua University and Zhongguancun Lab)

Enhancing Website Fingerprinting Attacks against Traffic Drift
Xinhao Deng (INSC, Tsinghua University and Ant Group), Yixiang Zhang (INSC, Tsinghua University), Qi Li (INSC, Tsinghua University, State Key Laboratory of Internet Architecture, Tsinghua University and Zhongguancun Laboratory), Zhuotao Liu (INSC, Tsinghua University and Zhongguancun Laboratory), Yabo Wang (DCST, Tsinghua University), Ke Xu (DCST, Tsinghua University, State Key Laboratory of Internet Architecture, Tsinghua University and Zhongguancun Laboratory)

NetRadar: Enabling Robust Carpet Bombing DDoS Detection
Junchen Pan (Tsinghua University), Lei Zhang (Zhongguancun Laboratory), Xiaoyong Si (Tencent Technology (Shenzhen)), Jie Zhang (Tsinghua University), Xinggong Zhang (Peking University), Yong Cui (Tsinghua University)

WiFinger: Fingerprinting Noisy IoT Event Traffic Using Packet-level Sequence Matching
Ronghua Li (The Hong Kong Polytechnic University), Shinan Liu (The University of Hong Kong), Haibo Hu (The Hong Kong Polytechnic University, PolyU Research Centre for Privacy and Security Technologies in Future Smart Systems), Qingqing Ye (The Hong Kong Polytechnic University), Nick Feamster (University of Chicago)

Session 1B: AI Security The Model Strikes Back

ThinkTrap: Denial-of-Service Attacks against Black-box LLM Services via Infinite Thinking
Yunzhe Li (Shanghai Jiao Tong University), Jianan Wang (Shanghai Jiao Tong University), Hongzi Zhu (Shanghai Jiao Tong University), James Lin (Shanghai Jiao Tong University), Shan Chang (Donghua University), Minyi Guo (Shanghai Jiao Tong University)

NeuroStrike: Neuron-Level Attacks on Aligned LLMs
Lichao Wu (Technical University of Darmstadt), Sasha Behrouzi (Technical University of Darmstadt), Mohamadreza Rostami (Technical University of Darmstadt), Maximilian Thang (Technical University of Darmstadt), Stjepan Picek (University of Zagreb & Radboud University), Ahmad-Reza Sadeghi (Technical University of Darmstadt)

In-Context Probing for Membership Inference in Fine-Tuned Language Models
Zhexi Lu (Rensselaer Polytechnic Institute), Hongliang Chi (Rensselaer Polytechnic Institute), Nathalie Baracaldo (IBM Research), Swanand Ravindra Kadhe (IBM Research), Yuseok Jeon (Korea University), Lei Yu (Rensselaer Polytechnic Institute)

Characterizing the Implementation of Censorship Policies in Chinese LLM Services
Anna Ablove (University of Michigan), Shreyas Chandrashekaran (University of Michigan), Xiao Qiang (University of California at Berkeley), Roya Ensafi (University of Michigan)

Session 1C: Distributed Systems & Security Four Horsemen of the Scale-pocalypse

Idioms: A Simple and Effective Framework for Turbo-Charging Local Neural Decompilation with Well-Defined Types
Luke Dramko (Carnegie Mellon University), Claire Le Goues (Carnegie Mellon University), Edward J. Schwartz (Carnegie Mellon University)

HoneySat: A Network-based Satellite Honeypot Framework
Efrén López-Morales (New Mexico State University), Ulysse Planta (CISPA Helmholtz Center for Information Security), Gabriele Marra (CISPA Helmholtz Center for Information Security), Carlos Gonzalez-Cortes (Universidad de Santiago de Chile and German Aerospace Center (DLR)), Jacob Hopkins (Texas A&M University - Corpus Christi), Majid Garoosi (CISPA Helmholtz Center for Information Security), Elías Obreque (Universidad de Chile), Carlos Rubio-Medrano (Texas A&M University - Corpus Christi), Ali Abbasi (CISPA Helmholtz Center for Information Security)

Pando: Extremely Scalable BFT Based on Committee Sampling
Xin Wang (Tsinghua University and State Key Laboratory of Cryptography and Digital Economy Security), Haochen Wang (Tsinghua University), Haibin Zhang (Yangtze Delta Region Institute of Tsinghua University, Zhejiang), Sisi Duan (Tsinghua University, Zhongguancun Laboratory, Shandong Institute of

Blockchains and State Key Laboratory of Cryptography and Digital Economy Security)

Janus: Enabling Expressive and Efficient ACLs in High-speed RDMA Clouds
Ziteng Chen (Southeast University), Menghao Zhang (Beihang University), Jiahao Cao (Tsinghua University & Quan Cheng Laboratory), Xuzheng Chen (Zhejiang University), Qiyang Peng (Beihang University), Shicheng Wang (Unaffiliated), Guanyu Li (Unaffiliated), Mingwei Xu (Quan Cheng Laboratory & Tsinghua University & Southeast University)

Session 1D: Microarchitectural Security Caches to Ashes

SNPeek: Side-Channel Analysis for Privacy Applications on Confidential VMs
Ruiyi Zhang (CISPA Helmholtz Center for Information Security and Google), Albert Cheu (Google), Adria Gascon (Google), Daniel Moghimi (Google), Phillipp Schoppmann (Google), Michael Schwarz (CISPA Helmholtz Center for Information Security), Octavian Suciu (Google)

Revisiting Differentially Private Hyper-parameter Tuning
Zihang Xiang (KAUST), Tianhao Wang (University of Virginia), Cheng-Long Wang (KAUST), Di Wang (KAUST)

Eviction Notice: Reviving and Advancing Page Cache Attacks
Sudheendra Raghav Neela (Graz University of Technology), Jonas Juffinger (Graz University of Technology), Lukas Maar (Graz University of Technology), Daniel Gruss (Graz University of Technology)

FLIPPYRAM: A Large-Scale Study of Rowhammer Prevalence
Martin Heckel (Hof University of Applied Sciences), Nima Sayadi (Hof University of Applied Sciences), Jonas Juffinger (Graz University of Technology), Carina Fiedler (Graz University of Technology), Daniel Gruss (Graz University of Technology), Florian Adamsky (Hof University of Applied Sciences)

Session 2A: Cross-Domain Attacks & Defenses Walls Are Suggestions

BLERP: BLE Re-Pairing Attacks and Defenses
Tommaso Sacchetti (EURECOM), Daniele Antonioli (EURECOM)

Breaking Isolation: A New Perspective on Hypervisor Exploitation via Cross-Domain Attacks
Gaoning Pan (Hangzhou Dianzi University & Zhejiang Provincial Key Laboratory of Sensitive Data Security and Confidentiality Governance), Yiming Tao (Zhejiang University), Qinying Wang (EPFL and Zhejiang University), Chunming Wu (Zhejiang University), Mingde Hu (Hangzhou Dianzi University & Zhejiang Provincial Key Laboratory of Sensitive Data Security and Confidentiality Governance), Yizhi Ren (Hangzhou Dianzi University & Zhejiang Provincial Key Laboratory of Sensitive Data Security and Confidentiality Governance), Shouling Ji (Zhejiang University)

Memory Band-Aid: A Principled Rowhammer Defense-in-Depth
Carina Fiedler (Graz University of Technology), Jonas Juffinger (Graz University of Technology), Sudheendra Raghav Neela (Graz University of Technology),

Martin Heckel (Hof University of Applied Sciences), Hannes Weissteiner (Graz University of Technology), Abdullah Giray Yağlıkçı (ETH Zürich), Florian Adamsky (Hof University of Applied Sciences), Daniel Gruss (Graz University of Technology)

Mirage: Private, Mobility-based Routing for Censorship Evasion
Zachary Ratliff (Harvard University), Ruoxing (David) Yang (Georgetown University), Avery Bai (Georgetown University), Harel Berger (Ariel University), Micah Sherr (Georgetown University), James Mickens (Harvard University)

Session 2B: Trusted Execution & Privacy Gone in 60 Milliseconds

Automated Code Annotation with LLMs for Establishing TEE Boundaries
Varun Gadey (University of Würzburg), Melanie Melanie Gotz (University of Würzburg), Christoph Sendner (University of Würzburg), Sampo Sovio (Huawei Technologies), Alexandra Dmitrienko (University of Wuerzburg)

SoK: Analysis of Accelerator TEE Designs
Chenxu Wang (Research Institute of Trustworthy Autonomous Systems, Southern University of Science and Technology, China, Department of Computer Science and Engineering, Southern University of Science and Technology, China and Department of Computing, The Hong Kong Polytechnic University, China), Junjie Huang (Department of Computer Science and Engineering, Southern University of Science and Technology, China), Yujun Liang (Department of Computer Science and Engineering, Southern University of Science and Technology, China), Xuanyao Peng (Department of Computer Science and Engineering, Southern University of Science and Technology, China and University of Chinese Academy of Sciences, China), Yuqun Zhang (Department of Computer Science and Engineering, Southern University of Science and Technology, China), Fengwei Zhang (Department of Computer Science and Engineering, Southern University of Science and Technology, China and Research Institute of Trustworthy Autonomous Systems, Southern University of Science and Technology, China), Jiannong Cao (Department of Computing, The Hong Kong Polytechnic University, China), Hang Lu (University of Chinese Academy of Sciences, China), Rui Hou (State Key Laboratory of Cyberspace Security Defense, IIE, Chinese Academy of Sciences, China and University of Chinese Academy of Sciences, China), Shoumeng Yan (Ant Group), Tao Wei (Ant Group), Zhengyu He (Ant Group)

PrivCode: When Code Generation Meets Differential Privacy
Zheng Liu (University of Virginia), Chen Gong (University of Virginia), Terry Yue Zhuo (Monash University and CSIRO's Data61), Kecen Li (University of Virginia), Weichen Yu (Carnegie Mellon University), Matt Fredrikson (Carnegie Mellon University), Tianhao Wang (University of Virginia)

UIEE: Secure and Efficient User-space Isolated Execution Environment for Embedded TEE Systems
Huaiyu Yan (Southeast University), Zhen Ling (Southeast University), Xuandong Chen (Southeast University), Xinhui Shao (Southeast University, City University of Hong Kong), Yier Jin (University of Science and Technology of China), Haobo

Li (Southeast University), Ming Yang (Southeast University), Ping Jiang (Southeast University), Junzhou Luo (Southeast University, Fuyao University of Science and Technology)

Session 2C: Applied Cryptography The Hashing Dead

Select-Then-Compute: Encrypted Label Selection and Analytics over Distributed Datasets using FHE

Nirajan Koirala (University of Notre Dame), Seunghun Paik (Hanyang University), Sam Martin (University of Notre Dame), Helena Berens (University of Notre Dame), Tasha Januszewicz (University of Notre Dame), Jonathan Takeshita (Old Dominion University), Jae Hong Seo (Hanyang University), Taeho Jung (University of Notre Dame)

cwPSU: Efficient Unbalanced Private Set Union via Constant-weight Codes

Qingwen Li (Xidian University), Song Bian (Beihang University), Hui Li (Xidian University)

Robust Fraud Transaction Detection: A Two-Player Game Approach

Qi Tan (College of Computer Science and Software Engineering, Shenzhen University), Yi Zhao (School of Cyberspace Science and Technology, Beijing Institute of Technology), Laizhong Cui (College of Computer Science and Software Engineering, Shenzhen University), Qi Li (Institute for Network Science and Cyberspace, Tsinghua University), Ming Zhu (Department of Computer Science and Technology, Tsinghua University), Xing Fu (Ant Group), Weiqiang Wang (Ant Group), Xiaotong Lin (Ant Group), Ke Xu (Department of Computer Science and Technology, Tsinghua University)

Cirrus: Performant and Accountable Distributed SNARK

Wenhao Wang (Yale University, IC3), Fangyan Shi (Tsinghua University), Dani Vilardell (Cornell University, IC3), Fan Zhang (Yale University, IC3)

Session 2D: Web & Content Security Click Wars: A New Hope

Paladin: Defending LLM-enabled Phishing Emails with a New Trigger-Tag Paradigm

Yan Pang (University of Virginia), Wenlong Meng (University of Virginia), Xiaojing Liao (Indiana University Bloomington), Tianhao Wang (University of Virginia)

Beyond Jailbreak: Unveiling Risks in LLM Applications Arising from Blurred Capability Boundaries

Yunyi Zhang (Tsinghua University), Shibo Cui (Tsinghua University), Baojun Liu (Tsinghua University), Jingkai Yu (Tsinghua University), Min Zhang (National University of Defense Technology), Fan Shi (National University of Defense Technology), Han Zheng (TrustAI Pte. Ltd.)

Incident Response Planning Using a Lightweight Large Language Model with Reduced Hallucination

Kim Hammar (Department of Electrical and Electronic Engineering, University of Melbourne, Australia), Tansu Alpcan (Department of Electrical and Electronic Engineering, University of Melbourne, Australia), Emil C. Lupu (Department of Computing, Imperial College London, United Kingdom)

Session 3A: Systems Security Kernel Panic at the Disco

IoTBec: An Accurate and Efficient Recurring Vulnerability Detection Framework for Black Box IoT devices

Haoran Yang (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Jiaming Guo (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Shuangning Yang (School of Internet, Anhui University, China), Guoli Zhao (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Qingqi Liu (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Chi Zhang (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Zhenlu Tan (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Lixiao Shan (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Qihang Zhou (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Mengting Zhou (Institute of Information Engineering, Chinese Academy of Sciences, China), Jianwei Tai (School of Internet, Anhui University, China), Xiaoqi Jia (Institute of Information Engineering, Chinese Academy of Sciences, China and School of Cyber Security, University of Chinese Academy of Sciences, China)

FirmCross: Detecting Taint-style Vulnerabilities in Modern C-Lua Hybrid Web Services of Linux-based Firmware

Runhao Liu (National University of Defense Technology), Jiarun Dai (Fudan University), Haoyu Xiao (Fudan University), Yuan Zhang (Fudan University), Yeqi Mou (National University of Defense Technology), Lukai Xu (National University of Defense Technology), Bo Yu (National University of Defense Technology), Baosheng Wang (National University of Defense Technology), Min Yang (Fudan University)

Trust Me, I Know This Function: Hijacking LLM Static Analysis using Bias

Shir Bernstein (Ben-Gurion University of the Negev, Israel), David Beste (CISPA Helmholtz Center for Information Security, Germany), Daniel Ayzenshteyn (Ben-Gurion University of the Negev, Israel), Lea Schönherr (CISPA Helmholtz Center for Information Security, Germany), Yisroel Mirsky (Ben-Gurion University of the Negev, Israel)

TranSPArent: Taint-style Vulnerability Detection in Generic Single Page Applications through Automated Framework Abstraction

Senapati Diwangkara (Johns Hopkins University), Yinzhi Cao (Johns Hopkins University)

Session 3B: AI Security No Country for Old Prompts

Chimera: Harnessing Multi-Agent LLMs for Automatic Insider Threat Simulation
Jiongchi Yu (Singapore Management University), Xiaofei Xie (Singapore Management University), Qiang Hu (Tianjin University), Yuhan Ma (Tianjin University), Ziming Zhao (Zhejiang University)

Les Dissonances: Cross-Tool Harvesting and Polluting in Pool-of-Tools Empowered LLM Agents
Zichuan Li (University of Illinois Urbana-Champaign), Jian Cui (University of Illinois Urbana-Champaign), Xiaojing Liao (University of Illinois Urbana-Champaign), Luyi Xing (University of Illinois Urbana-Champaign)

Achieving Interpretable DL-based Web Attack Detection through Malicious Payload Localization
Peiyang Li (INSC and the State Key Laboratory of Internet Architecture, Tsinghua University and Ant Group), Fukun Mei (INSC and the State Key Laboratory of Internet Architecture, Tsinghua University), Ye Wang (INSC and the State Key Laboratory of Internet Architecture, Tsinghua University), Zhuotao Liu (INSC and the State Key Laboratory of Internet Architecture, Tsinghua University), Ke Xu (DCST and the State Key Laboratory of Internet Architecture, Tsinghua University and Zhongguancun Laboratory), Chao Shen (Xi'an Jiaotong University), Qian Wang (Wuhan University), Qi Li (INSC and the State Key Laboratory of Internet Architecture, Tsinghua University and Zhongguancun Laboratory)

Attention is All You Need to Defend Against Indirect Prompt Injection Attacks in LLMs
Yinan Zhong (Zhejiang University), Qianhao Miao (Zhejiang University), Yanjiao Chen (Zhejiang University), Jiangyi Deng (Zhejiang University), Yushi Cheng (Zhejiang University), Wenyuan Xu (Zhejiang University)

Session 3C: Apps and Cloud Security Prompt Hard with a Vengeance

ACE: A Security Architecture for LLM-Integrated App Systems
Evan Li (Northeastern University), Tushin Mallick (Northeastern University), Evan Rose (Northeastern University), William Robertson (Northeastern University), Alina Oprea (Northeastern University), Cristina Nita-Rotaru (Northeastern University)

Better Safe than Sorry: Uncovering the Insecure Resource Management in App-in-App Cloud Services
Yizhe Shi (Fudan University), Zhemin Yang (Fudan University), Dingyi Liu (Fudan University), Kangwei Zhong (Fudan University), Jiarun Dai (Fudan University), Min Yang (Fudan University)

Side-channel Inference of User Activities in AR/VR Using GPU Profiling
Seonghun Son (Iowa State University), Chandrika Mukherjee (Purdue University), Reham Mohamed Aburas (American University of Sharjah), Berk Gulmezoglu (Iowa State University), Z. Berkay Celik (Purdue University)

MVPNalyzer: An Investigative Framework for Auditing the Security & Privacy of Mobile VPNs

Wayne Wang (University of Michigan), Aaron Ortwein (University of Michigan), Enrique Sobrados (University of New Mexico), Robert Stanley (University of Michigan), Piyush Kumar Sharma (University of Michigan, IIT Delhi), Afsah Anwar (University of New Mexico), Roya Ensafi (University of Michigan)

Session 3D: Distributed & Secure Computation The Fellowship of the MPC

HOUSTON: Real-Time Anomaly Detection of Attacks against Ethereum DeFi Protocols

Dongyu Meng (University of California, Santa Barbara), Fabio Gritti (University of California, Santa Barbara), Robert McLaughlin (University of California, Santa Barbara), Nicola Ruaro (University of California, Santa Barbara), Ilya Grishchenko (University of Toronto), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California, Santa Barbara)

Indicator of Benignity: An Industry View of False Positive in Malicious Domain Detection and its Mitigation

Daiping Liu (Palo Alto Networks, Inc.), Danyu Sun (University of California, Irvine), Zhenhua Chen (Palo Alto Networks, Inc.), Shu Wang (Palo Alto Networks, Inc.), Zhou Li (University of California, Irvine)

VDORAM: Towards a Random Access Machine with Both Public Verifiability and Distributed Obliviousness

Huayi Qi (School of Computer Science and Technology, Shandong University, Qingdao, Shandong, China and Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing, China), Minghui Xu (School of Computer Science and Technology, Shandong University, Qingdao, Shandong, China), Xiaohua Jia (Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong SAR, China), Xiuzhen Cheng (School of Computer Science and Technology, Shandong University, Qingdao, Shandong, China)

RoundRole: Unlocking the Efficiency of Multi-party Computation with Bandwidth-aware Execution

Xiaoyu Fan (Tsinghua University and Shanghai Qi Zhi Institute), Kun Chen (Ant Group), Jiping Yu (Tsinghua University), Xin Liu (Tsinghua University), Yunyi Chen (Tsinghua University), Wei Xu (Tsinghua University and Shanghai Qi Zhi Institute)

Session 4A: Privacy & Measurement Where's Waldo's Data

When Focus Enhances Utility: Target Range LDP Frequency Estimation and Unknown Item Discovery

Bo Jiang (TikTok Inc.), Wanrong Zhang (TikTok Inc.), Donghang Lu (TikTok Inc.), Jian Du (TikTok Inc.), Qiang Yan (TikTok Inc.)

Augmented Shuffle Differential Privacy Protocols for Large-Domain Categorical and Key-Value Data

Takao Murakami (ISM/AIST/RIKEN AIP), Yuichi Sei (UEC), Reo Eriguchi (AIST)

PrivATE: Differentially Private Average Treatment Effect Estimation for Observational Data

Quan Yuan (Zhejiang University and University of Virginia), Xiaochen Li (University of North Carolina at Greensboro), Linkang Du (Xi'an Jiaotong University), Min Chen (Vrije Universiteit Amsterdam), Mingyang Sun (Peking University), Yunjun Gao (Zhejiang University), Shibo He (Zhejiang University), Jiming Chen (Zhejiang University and Hangzhou Dianzi University), Zhikun Zhang (Zhejiang University)

Convergent Privacy Framework for Multi-layer GNNs through Contractive Message Passing

Yu Zheng (University of California, Irvine), Chenang Li (University of California, Irvine), Zhou Li (University of California, Irvine), Qingsong Wang (University of California, San Diego)

Session 4B: Systems Security Seal Team Sixteen

NetCap: Data-Plane Capability-Based Defense Against Token Theft in Network Access

Osama Bajaber (Virginia Tech), Bo Ji (Virginia Tech), Peng Gao (Virginia Tech)

On the Security Risks of Memory Adaptation and Augmentation in Data-plane DoS Mitigation

Hocheol Nam (KAIST), Daehyun Lim (KAIST), Huancheng Zhou (Texas A&M University), Guofei Gu (Texas A&M University), Min Suk Kang (KAIST)

Beyond Conventional Triggers: Auto-Contextualized Covert Triggers for Android Logic Bombs

Ye Wang (Department of Electrical Engineering and Computer Science, Institute for Information Sciences, The University of Kansas), Bo Luo (Department of Electrical Engineering and Computer Science, Institute for Information Sciences, The University of Kansas), Fengjun Li (Department of Electrical Engineering and Computer Science, Institute for Information Sciences, The University of Kansas)

SAGA: A Security Architecture for Governing AI Agentic Systems

Georgios Syros (Northeastern University), Anshuman Suri (Northeastern University), Jacob Ginesin (Northeastern University), Cristina Nita-Rotaru (Northeastern University), Alina Oprea (Northeastern University)

Session 4C: Web & Content Security Spider Man: No Way to Phish

From Obfuscated to Obvious: A Comprehensive JavaScript Deobfuscation Tool for Security Analysis

Dongchao Zhou (Beijing University of Post and Telecommunication and QI-ANXIN Technology Research Institute), Lingyun Ying (QI-ANXIN Technology Research Institute), Huajun Chai (QI-ANXIN Technology Research Institute), Dongbin Wang (Beijing University of Post and Telecommunication)

Cross-Boundary Mobile Tracking: Exploring Java-to-JavaScript Information Diffusion in WebViews

Sohom Datta (North Carolina State University, USA), Michalis Diamantaris (TTechnical University of Crete, Greece), Ahsan Zafar (North Carolina State

University, USA), Junhua Su (North Carolina State University, USA), Anupam Das (North Carolina State University, USA), Jason Polakis (University of Illinois Chicago, USA), Alexandros Kapravelos (North Carolina State University, USA)

LLMBisect: Breaking Barriers in Bug Bisection with A Comparative Analysis Pipeline
Zheng Zhang (University of California, Riverside), Haonan Li (University of California, Riverside), Xingyu Li (University of California, Riverside), Hang Zhang (Indiana University Bloomington), Zhiyun Qian (University of California, Riverside)

Prompt Injection Attack to Tool Selection in LLM Agents
Jiawen Shi (Huazhong University of Science and Technology), Zenghui Yuan (Huazhong University of Science and Technology), Guiyao Tie (Huazhong University of Science and Technology), Pan Zhou (Huazhong University of Science and Technology), Neil Zhenqiang Gong (Duke University), Lichao Sun (Lehigh University)

Session 4D: AI Security The Good, the Bad, and the Adversarial

Character-Level Perturbations Disrupt LLM Watermarks
Zhaoxi Zhang (University of Technology Sydney), Xiaomei Zhang (Griffith University), Yanjun Zhang (University of Technology Sydney), He Zhang (RMIT University), Shirui Pan (Griffith University), Bo Liu (University of Technology Sydney), Asif Gill (University of Technology Sydney Australia), Leo Yu Zhang (Griffith University)

Dataset Reduction and Watermark Removal via Self-supervised Learning for Model Extraction Attack
Hao Luan (Institute of Big Data, Fudan University, Shanghai, China and College of Computer Science and Artificial Intelligence, Fudan University, Shanghai, China), Xue Tan (Institute of Big Data, Fudan University, Shanghai, China and College of Computer Science and Artificial Intelligence, Fudan University, Shanghai, China), Zhiheng Li (School of Control Science and Engineering, Shandong University, Jinan, China), Jun Dai (Department of Computer Science, Worcester Polytechnic Institute, MA, USA), Xiaoyan Sun (Department of Computer Science, Worcester Polytechnic Institute, MA, USA), Ping Chen (Institute of Big Data, Fudan University, Shanghai, China and Purple Mountain Laboratories, Nanjing, China)

Unshaken by Weak Embedding: Robust Probabilistic Watermarking for Dataset Copyright Protection
Shang Wang (University of Technology Sydney, Australia), Tianqing Zhu (City University of Macau, Macau SAR, China), Dayong Ye (City University of Macau, Macau SAR, China), Hua Ma (Data61, CSIRO, Australia), Bo Liu (University of Technology Sydney, Australia), Ming Ding (Data61, CSIRO, Australia), Shengfang Zhai (National University of Singapore, Singapore), Yansong Gao (School of Cyber Science and Engineering, Southeast University, China)

Benchmarking and Understanding Safety Risks in AI Character Platforms
Yiluo Wei (The Hong Kong University of Science and Technology (Guangzhou)), Peixian Zhang (The Hong Kong University of Science and Technology

(Guangzhou)), Gareth Tyson (The Hong Kong University of Science and Technology (Guangzhou))

Session 5A: Systems Security Process and the Furious

SACK: Systematic Generation of Function Substitution Attacks Against Control-Flow Integrity

Zhechang Zhang (The Pennsylvania State University), Hengkai Ye (The Pennsylvania State University), Song Liu (University of Delaware), Hong Hu (The Pennsylvania State University)

DirtyFree: Simplified Data-Oriented Programming in the Linux Kernel

Yoochan Lee (Max Planck Institute for Security and Privacy), Hyuk Kwon (Theori, Inc.), Thorsten Holz (Max Planck Institute for Security and Privacy)

EXIA: Trusted Transitions for Enclaves via External-Input Attestation

Zhen Huang (Shanghai Jiao Tong University), Yidi Kao (Auburn University), Sanchuan Chen (Auburn University), Guoxing Chen (Shanghai Jiao Tong University), Yan Meng (Shanghai Jiao Tong University), Haojin Zhu (Shanghai Jiao Tong University)

LinkGuard: A Lightweight State-Aware Runtime Guard Against Link Following Attacks in Windows File System

Bocheng Xiang (Fudan University), Yuan Zhang (Fudan University), Hao Huang (Fudan university), Fengyu Liu (Fudan University), Youkun Shi (Fudan University)

Session 5B: Program Analysis & Fuzzing Fuzz Lightyear to Infinity

ProtocolGuard: Detecting Protocol Non-compliance Bugs via LLM-guided Static Analysis and Dynamic Verification

Xiangpu Song (School of Cyber Science and Technology, Shandong University), Longjia Pei (School of Cyber Science and Technology, Shandong University), Jianliang Wu (Simon Fraser University), Yingpei Zeng (Hangzhou Dianzi University), Gaoshuo He (School of Cyber Science and Technology, Shandong University), Chaoshun Zuo (Independent Researcher), Xiaofeng Liu (School of Cyber Science and Technology, Shandong University), Qingchuan Zhao (City University of Hong Kong), Shanqing Guo (School of Cyber Science and Technology, Shandong University, Shandong Key Laboratory of Artificial Intelligence Security and State Key Laboratory of Cryptography and Digital Economy Security, Shandong University)

Formal Analysis of BLE Secure Connection Pairing and Revelation of the PE Confusion Attack

Min Shi (Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University), Yongkang Xiao (Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University), Jing Chen (Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University), Kun He (Key Laboratory of

Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University), Ruiying Du (Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University), Meng Jia (Department of Computing, The Hong Kong Polytechnic University)

An LLM-Driven Fuzzing Framework for Detecting Logic Instruction Bugs in PLCs
Jiaxing Cheng (Institute of Information Engineering, CAS; SCS, UCAS Beijing, China), Ming Zhou (SCS, Nanjing University of Science and Technology Nanjing, Jiangsu, China), Haining Wang (ECE Virginia Tech Arlington, VA, USA), Xin Chen (Institute of Information Engineering, CAS; SCS, UCAS Beijing, China), Yuncheng Wang (Institute of Information Engineering CAS; SCS, UCAS Beijing, China), Yibo Qu (Institute of Information Engineering CAS; SCS, UCAS Beijing, China), Limin Sun (Institute of Information Engineering CAS; SCS, UCAS Beijing, China)

What Do They Fix? LLM-Aided Categorization of Security Patches for Critical Memory Bugs
Xingyu Li (UC Riverside), Juefei Pu (UC Riverside), Yifan Wu (UC Riverside), Xiaochen Zou (UC Riverside), Shitong Zhu (UC Riverside), Qiushi Wu (IBM), Zheng Zhang (UC Riverside), Joshua Hsu (UC Riverside), Yue Dong (UC Riverside), Zhiyun Qian (UC Riverside), Kangjie Lu (University of Minnesota), Trent Jaeger (UC Riverside), Michael De Lucia (U.S. Army Research Laboratory), Srikanth V. Krishnamurthy (UC Riverside)

Session 5C: Multimedia Forensics CSI: JPEG Unit

ViGText: Deepfake Image Detection with Vision-Language Model Explanations and Graph Neural Networks
Ahmad ALBarqawi (New Jersey Institute of Technology, Newark, NJ, USA), Mahmoud Nazzal (Old Dominion University, Norfolk, VA, USA), Issa Khalil (Qatar Computing Research Institute (QCRI), HBKU, Doha, Qatar), Abdallah Khreishah (New Jersey Institute of Technology, Newark, NJ, USA), NhatHai Phan (New Jersey Institute of Technology, Newark, NJ, USA)

Light2Lie: Detecting Deepfake Images Using Physical Reflectance Laws
Kavita Kumari (Technical University of Darmstadt), Sasha Behrouzi (Technical University of Darmstadt), Alessandro Pegoraro (Technical University of Darmstadt), Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Rethinking Fake Speech Detection: A Generalized Framework Leveraging Spectrogram Magnitude
Zihao Liu (Iowa State University), Aobo Chen (Iowa State University), Yan Zhang (Iowa State University), Wensheng Zhang (Iowa State University), Chenglin Miao (Iowa State University)

CAT: Can Trust be Predicted with Context-Awareness in Dynamic Heterogeneous Networks?
Jie Wang (State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University), Zheng Yan (State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University

and Hangzhou Institute of Technology, Xidian University), Jiahe Lan (State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University), Xuyan Li (Hangzhou Institute of Technology, Xidian University), Elisa Bertino (Department of Computer Science, Purdue University)

Session 5D: Microarchitectural Security Cache Me If You Can

When Cache Poisoning Meets LLM Systems: Semantic Cache Poisoning and Its Countermeasures

Guanlong Wu (SUSTech), Taojie Wang (SUSTech), Yao Zhang (ByteDance Inc.), Zheng Zhang (SUSTech), Jianyu Niu (SUSTech), Ye Wu (ByteDance Inc.), Yinqian Zhang (SUSTech)

Shadow in the Cache: Unveiling and Mitigating Privacy Risks of KV-cache in LLM Inference

Zhifan Luo (State Key Laboratory of Blockchain and Data Security, Zhejiang University), Shuo Shao (State Key Laboratory of Blockchain and Data Security, Zhejiang University), Su Zhang (Huawei Technology), Lijing Zhou (Huawei Technology), Yuke Hu (State Key Laboratory of Blockchain and Data Security, Zhejiang University), Chenxu Zhao (State Key Laboratory of Blockchain and Data Security, Zhejiang University), Zhihao Liu (State Key Laboratory of Blockchain and Data Security, Zhejiang University), Zhan Qin (State Key Laboratory of Blockchain and Data Security, Zhejiang University and Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security)

Should I Trust You? Rethinking the Principle of Zone-Based Isolation DNS Bailiwick Checking

Yuxiao Wu (Institute for Network Sciences and Cyberspace, BNRist, Tsinghua University), Yunyi Zhang (Tsinghua University), Chaoyi Lu (Zhongguancun Laboratory), Baojun Liu (Tsinghua University and Zhongguancun Laboratory)

Cross-Cache Attacks for the Linux Kernel via PCP Massaging

Claudio Migliorelli (IBM Research Europe - Zurich), Andrea Mambretti (IBM Research Europe - Zurich), Alessandro Sorniotti (IBM Research Europe - Zurich), Vittorio Zaccaria (Politecnico di Milano), Anil Kurmus (IBM Research Europe - Zurich)

Session 6A: Privacy & Measurement The Sound of (Meta)Data

Memory Backdoor Attacks on Neural Networks

Eden Luzon (Ben-Gurion University, Institute of Software Systems and Security), Guy Amit (Ben-Gurion University, Institute of Software Systems and Security), Roy Weiss (Ben-Gurion University, Institute of Software Systems and Security), Torsten Krauß (University of Würzburg), Alexandra Dmitrienko (University of Würzburg), Yisroel Mirsky (Ben-Gurion University, Institute of Software Systems and Security)

AirSnitch: Demystifying and Breaking Client Isolation in Wi-Fi Networks

Xin'an Zhou (University of California, Riverside), Juefei Pu (University of California, Riverside), Zhutian Liu (University of California, Riverside), Zhiyun Qian (University of California, Riverside), Zhaowei Tan (University of California,

Riverside), Srikanth V. Krishnamurthy (University of California, Riverside), Mathy Vanhoef (DistriNet, KU Leuven)

Entente: Cross-silo Intrusion Detection on Network Log Graphs with Federated Learning
Jiacen Xu (Microsoft), Chenang Li (University of California, Irvine), Yu Zheng (University of California, Irvine), Zhou Li (University of California, Irvine)

SVDefense: Effective Defense against Gradient Inversion Attacks via Singular Value Decomposition
Chenxiang Luo (City University of Hong Kong), David K.Y. Yau (Singapore University of Technology and Design), Qun Song (City University of Hong Kong)

Session 6B: Systems Security The Permission: Impossible

Pitfalls for Security Isolation in Multi-CPU Systems
Simeon Hoffmann (CISPA Helmholtz Center for Information Security), Nils Ole Tippenhauer (CISPA Helmholtz Center for Information Security)

HyperMirage: Direct State Manipulation in Hybrid Virtual CPU Fuzzing
Manuel Andreas (Technical University of Munich), Fabian Specht (Technical University of Munich), Marius Momeu (Technical University of Munich)

IsolatOS: Detecting Double Fetch Bugs in COTS RTOS by Re-enabling Kernel Isolation
Yingjie Cao (Sun Yat-sen University and The Hong Kong Polytechnic University), Xiaogang Zhu (Adelaide University), Dean Sullivan (University of New Hampshire, US), Haowei Yang, Lei Xue (Sun Yat-sen University), Xian Li (Swinburne University of Technology, Australia), Chenxiong Qian (University of Hong Kong, China), Minrui Yan (Swinburne University of Technology, Australia), Xiapu Luo (The Hong Kong Polytechnic University)

PhantomMap: GPU-Assisted Kernel Exploitation
Jiayi Hu (Zhejiang University), Qi Tang (Jilin University), Xingkai Wang (Zhejiang University), Jinmeng Zhou (Zhejiang University), Rui Chang (Zhejiang University), Wenbo Shen (Zhejiang University)

Session 6C: AI Security AIs Wide Shut

DNN Latency Sequencing: Extracting DNN Architectures from Intel SGX Enclaves with Single-Stepping Attacks
Minkyung Park (University of Texas at Dallas), Zelun Kong (University of Texas at Dallas), Dave (Jing) Tian (Purdue University), Z. Berkay Celik (Purdue University), Chung Hwan Kim (University of Texas at Dallas)

Peering Inside the Black-Box: Long-Range and Scalable Model Architecture Snooping via GPU Electromagnetic Side-Channel
Rui Xiao (Zhejiang University), Sibo Feng (Zhejiang University), Soundarya Ramesh (National University of Singapore), Jun Han (KAIST), Jinsong Han (Zhejiang University)

Achieving Zen: Combining Mathematical and Programmatic Deep Learning Model Representations for Attribution and Reuse

David Oygenblik (Georgia Institute of Technology), Dinko Dermendzhiev (Georgia Institute of Technology), Filippos Sofias (Georgia Institute of Technology), Mingxuan Yao (Georgia Institute of Technology), Haichuan Xu (Georgia Institute of Technology), Runze Zhang (Georgia Institute of Technology), Jeman Park (Kyung Hee University), Amit Kumar Sikder (Iowa State University), Brendan Saltaformaggio (Georgia Institute of Technology)

Session 6D: Wireless Security Key Largo

XR Devices Send WiFi Packets When They Should Not: Cross-Building Keylogging Attacks via Non-Cooperative Wireless Sensing

Christopher Vattheuer (University of California, Los Angeles (UCLA)), Justin Feng (University of California, Los Angeles (UCLA)), Hossein Khalili (University of California, Los Angeles (UCLA)), Nader Sehatbakhsh (University of California, Los Angeles (UCLA)), Omid Abari (University of California, Los Angeles (UCLA))

From Perception to Protection: A Developer-Centered Study of Security and Privacy Threats in Extended Reality (XR)

Kunlin Cai (University of California, Los Angeles), Jinghuai Zhang (University of California, Los Angeles), Ying Li (University of California, Los Angeles), Zhiyuan Wang (University of Virginia), Xun Chen (Independent Researcher), Tianshi Li (Northeastern University), Yuan Tian (University of California, Los Angeles)

PhantomMotion: Laser-Based Motion Injection Attacks on Wireless Security Surveillance Systems

Yan He (University of Oklahoma), Guanchong Huang (University of Oklahoma), Song Fang (University of Oklahoma)

Unknown Target: Uncovering and Detecting Novel In-Flight Attacks to Collision Avoidance (TCAS)

Giacomo Longo (CASD - University School of Advanced Defense Studies, Rome, Italy), Giacomo Ratto (CASD - University School of Advanced Defense Studies, Rome, Italy), Alessio Merlo (CASD - University School of Advanced Defense Studies, Rome, Italy), Enrico Russo (DIBRIS - University of Genova, Genova, Italy)

Session 7A: Network Security Lord of the Pings

CryptPEFT: Efficient and Private Neural Network Inference via Parameter-Efficient Fine-Tuning

Saisai Xia (State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS and School of Cyber Security, University of Chinese Academy of Sciences), Wenhao Wang (State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS and School of Cyber Security, University of Chinese Academy of Sciences), Zihao Wang (Nanyang Technological University), Yuhui Zhang (State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS and School of Cyber Security, University of Chinese Academy of Sciences), Yier Jin (University of Science and Technology of China), Dan Meng (State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering,

CAS and School of Cyber Security, University of Chinese Academy of Sciences), Rui Hou (State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS and School of Cyber Security, University of Chinese Academy of Sciences)

Kangaroo: A Private and Amortized Inference Framework over WAN for Large-Scale Decision Tree Evaluation

Wei Xu (Xidian University), Hui Zhu (Xidian University), Yandong Zheng (Xidian University), Song Bian (Beihang University), Ning Sun (Xidian University), Hao Yuan (Xidian University), Dengguo Feng (School of Cyber Science and Technology), Hui Li (Xidian University)

ProvGuard: Detecting SDN Control Policy Manipulation via Contextual Semantics of Provenance Graphs

Ziwen Liu (Beihang University), Jian Mao (Beihang University; Tianmushan Laboratory; Hangzhou Innovation Institute, Beihang University), Jun Zeng (National University of Singapore), Jiawei Li (Beihang University; National University of Singapore), Qixiao Lin (Beihang University), Jiahao Liu (National University of Singapore), Jianwei Zhuge (Tsinghua University; Zhongguancun Laboratory), Zhenkai Liang (National University of Singapore)

ANONYCALL: Enabling Native Private Calling in Mobile Networks

Hexuan Yu (Virginia Polytechnic Institute and State University), Chaoyu Zhang (Virginia Polytechnic Institute and State University), Yang Xiao (University of Kentucky), Angelos D. Keromytis (Georgia Institute of Technology), Y. Thomas Hou (Virginia Polytechnic Institute and State University), Wenjing Lou (Virginia Polytechnic Institute and State University)

CELLSHIFT: RTT-Aware Trace Transduction for Real-World Website Fingerprinting

Rob Jansen (U.S. Naval Research Laboratory)

Session 7B: Usable Security Password? I Hardly Know Her!

Connecting the Dots: An Investigative Study on Linking Private User Data Across Messaging Apps

Junkyu Kang (KAIST), Soyoung Lee (KAIST), Yonghwi Kwon (University of Maryland), Sooel Son (KAIST)

Hey there! You are using WhatsApp: Enumerating Three Billion Accounts for Security and Privacy

Gabriel K. Gegenhuber (University of Vienna, Faculty of Computer Science and UniVie Doctoral School Computer Science), Philipp E. Frenzel (SBA Research), Maximilian Günther (University of Vienna, Faculty of Computer Science), Johanna Ullrich (University of Vienna, Faculty of Computer Science), Aljosha Judmayer (University of Vienna, Faculty of Computer Science)

Anchors of Trust: A Usability Study on User Awareness, Consent, and Control in Cross-Device Authentication

Xin Zhang (Fudan University), Xiaohan Zhang (Fudan University), Huijun Zhou (Fudan University), Bo Zhao (Fudan University)

CHAMELEOSCAN: Demystifying and Detecting iOS Chameleon Apps via LLM-Powered UI Exploration
Hongyu Lin (Zhejiang University), Yicheng Hu (Zhejiang University), Haitao Xu (Zhejiang University), Yanchen Lu (Zhejiang University), Mengxia Ren (Zhejiang University), Shuai Hao (Old Dominion University), Chuan Yue (Colorado School of Mines), Zhao Li (Hangzhou Yugu Technology), Fan Zhang (Zhejiang University), Yixin Jiang (Electric Power Research Institute, CSG)

Session 7C: Privacy-Preserving Systems Trust Without Disclosure

PIRANHAS: PrIvacy-Preserving Remote Attestation in Non-Hierarchical Asynchronous Swarms
Jonas Hofmann (Technical University of Darmstadt), Philipp-Florens Lehwalder (Technical University of Darmstadt), Shahriar Ebrahimi (Alan Turing Institute), Parisa Hassanizadeh (IPPT PAN / University of Warwick), Sebastian Faust (Technical University of Darmstadt)

Cryptobazaar: Private Sealed-bid Auctions at Scale
Andrija Novakovic (Bain Capital Crypto), Alireza Kavousi (University College London), Kobi Gurkan (Bain Capital Crypto), Philipp Jovanovic (University College London)

MVP-ORAM: a Wait-free Concurrent ORAM for Confidential BFT Storage
Robin Vassantlal (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal), Hasan Heydari (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal), Bernardo Ferreira (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal), Alysson Bessani (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal)

Enhancing Legal Document Security and Accessibility with TAF
Renata Vaderna (Independent Researcher), Dušan Nikolić (University of Novi Sad), Patrick Zielinski (New York University), David Greisen (Open Law Library), BJ Ard (University of Wisconsin–Madison), Justin Cappos (New York University)

Session 7D: Malware & Reverse Engineering The Malware Ultimatum

Learning from Leakage: Database Reconstruction from Just a Few Multidimensional Range Queries
Peijie Li (Delft University of Technology), Huanhuan Chen (Delft University of Technology), Kaitai Liang (University of Turku and Delft University of Technology), Evangelia Anna Markatou (Delft University of Technology)

Enhancing Semantic-Aware Binary Diffing with High-Confidence Dynamic Instruction Alignment
Chengfeng Ye (The Hong Kong University of Science and Technology, China), Anshunkang Zhou (The Hong Kong University of Science and Technology, China), Charles Zhang (The Hong Kong University of Science and Technology, China)

DUALBREACH: Efficient Dual-Jailbreaking via Target-Driven Initialization and Multi-Target Optimization

Xinzhe Huang (Zhejiang University), Kedong Xiu (Zhejiang University), Tianhang Zheng (Zhejiang University), Churui Zeng (Zhejiang University), Wangze Ni (Zhejiang University), Zhan Qin (Zhejiang University), Kui Ren (Zhejiang University), Chun Chen (Zhejiang University)

Cease at the Ultimate Goodness: Towards Efficient Website Fingerprinting Defense via Iterative Mutual Information Minimization

Rong Wang (Southeast University), Zhen Ling (Southeast University), Guangchi Liu (Southeast University), Shaofeng Li (Southeast University), Junzhou Luo (Southeast University and Fuyao University of Science and Technology), Xinwen Fu (University of Massachusetts Lowell)

Session 8A: Malware & Reverse Engineering The Hitchhiker's Guide to the Binary

KnowHow: Automatically Applying High-Level CTI Knowledge for Interpretable and Accurate Provenance Analysis

Yuhan Meng (Key Laboratory of High-Confidence Software Technologies (MOE), School of Computer Science, Peking University), Shaofei Li (Key Laboratory of High-Confidence Software Technologies (MOE), School of Computer Science, Peking University), Jiaping Gui (School of Computer Science, Shanghai Jiao Tong University), Peng Jiang (Southeast University), Ding Li (Key Laboratory of High-Confidence Software Technologies (MOE), School of Computer Science, Peking University)

From Noise to Signal: Precisely Identify Affected Packages of Known Vulnerabilities in npm Ecosystem

Yingyuan Pu (QI-ANXIN Technology Research Institute), Lingyun Ying (QI-ANXIN Technology Research Institute), Yacong Gu (Tsinghua University, Tsinghua University-QI-ANXIN Group JCNS)

Automating Function-Level TARA for Automotive Full-Lifecycle Security

Yuqiao Yang (UESTC), Yongzhao Zhang (UESTC), Wenhao Liu (GoGoByte Technology), Jun Li (GoGoByte Technology), Pengtao Shi (GoGoByte Technology), DingYu Zhong (UESTC), Jie Yang (UESTC), Ting Chen (UESTC), Sheng Cao (UESTC), Yuntao Ren (UESTC), Yongyue Wu (UESTC), Xiaosong Zhang (UESTC)

Beyond Raw Bytes: Towards Large Malware Language Models

Luke Kurlandski (Rochester Institute of Technology, Rochester New York USA), Harel Berger (Ariel University, Israel), Yin Pan (Rochester Institute of Technology, Rochester New York USA), Matthew Wright (Rochester Institute of Technology, Rochester New York USA)

Session 8B: Program Analysis & Fuzzing Crash Bandicoot

Anota: Identifying Business Logic Vulnerabilities via Annotation-Based Sanitization

Meng Wang (CISPA Helmholtz Center for Information Security), Philipp Görz (CISPA Helmholtz Center for Information Security), Joschua Schilling (CISPA Helmholtz Center for Information Security), Keno Hassler (CISPA Helmholtz Center for Information Security), Liwei Guo (University of Electronic Science and

Technology), Thorsten Holz (Max Planck Institute for Security and Privacy), Ali Abbasi (CISPA Helmholtz Center for Information Security)

Discovering Blind-Trust Vulnerabilities in PLC Binaries via State Machine Recovery
Fangzhou Dong (Arizona State University), Arvind S Raj (Arizona State University), Efrén López-Morales (New Mexico State University), Siyu Liu (Arizona State University), Yan Shoshitaishvili (Arizona State University), Tiffany Bao (Arizona State University), Adam Doupé (Arizona State University), Muslum Ozgur Ozmen (Arizona State University), Ruoyu Wang (Arizona State University)

BunnyFinder: Finding Incentive Flaws for Ethereum Consensus
Rujia Li (Tsinghua University and State Key Laboratory of Cryptography and Digital Economy Security), Mingfei Zhang (Shandong University), Xueqian Lu (Independent Reseacher), Wenbo Xu (Blockchain Platform Division, Ant Group), Ying Yan (Blockchain Platform Division, Ant Group), Sisi Duan (Tsinghua University, Zhongguancun Laboratory, Shandong Institute of Blockchains and State Key Laboratory of Cryptography and Digital Economy Security)

ReFuzz: Reusing Tests for Processor Fuzzing with Contextual Bandits
Chen Chen (Texas A&M University, USA), Zaiyan Xu (Texas A&M University, USA), Mohamadreza Rostami (Technische Universitat Darmstadt, Germany), David Liu (Texas A&M University, USA), Dileep Kalathil (Texas A&M University, USA), Ahmad-Reza Sadeghi (Technische Universitat Darmstadt, Germany), Jeyavijayan (JV) Rajendran (Texas A&M University, USA)

Session 8C: AI Security Guardians of the Gradient

Was My Data Used for Training? Membership Inference in Open-Source LLMs via Neural Activations
Xue Tan (Institute of Big Data, Fudan University, Shanghai, China and College of Computer Science and Artificial Intelligence, Fudan University, Shanghai, China), Hao Luan (Institute of Big Data, Fudan University, Shanghai, China and College of Computer Science and Artificial Intelligence, Fudan University, Shanghai, China), Mingyu Luo (Institute of Big Data, Fudan University, Shanghai, China and College of Computer Science and Artificial Intelligence, Fudan University, Shanghai, China), Zhuyang Yu (Institute of Big Data, Fudan University, Shanghai, China and College of Computer Science and Artificial Intelligence, Fudan University, Shanghai, China), Jun Dai (Department of Computer Science, Worcester Polytechnic Institute, MA, USA), Xiaoyan Sun (Department of Computer Science, Worcester Polytechnic Institute, MA, USA), Ping Chen (Institute of Big Data, Fudan University, Shanghai, China and Purple Mountain Laboratories, Nanjing, China)

Cascading and Proxy Membership Inference Attacks
Yuntao Du (Purdue University), Jiacheng Li (Purdue University), Yuetian Chen (Purdue University), Kaiyuan Zhang (Purdue University), Zhizhen Yuan (Purdue University), Hanshen Xiao (Purdue University and NVIDIA Research), Bruno Ribeiro (Purdue University), Ninghui Li (Purdue University)

ExpShield: Safeguarding Web Text from Unauthorized Crawling and LLM Exploitation
Ruixuan Liu (Emory University), Toan Tran (Emory University), Tianhao Wang (University of Virginia), Hongsheng Hu (Shanghai Jiao Tong University), Shuo Wang (Shanghai Jiao Tong University), Li Xiong (Emory University)

OblInjection: Order-Oblivious Prompt Injection Attack to LLM Agents with Multi-source Data
Reachal Wang (Duke University), Yuqi Jia (Duke University), Neil Zhenqiang Gong (Duke University)

Session 8D: Network Security Packet to the Future

Lightweight Internet Bandwidth Allocation and Isolation with Fractional Fair Shares
Marc Wyss (ETH Zurich), Yih-Chun Hu (University of Illinois at Urbana-Champaign), Vincent Lenders (University of Luxembourg), Roland Meier (armasuisse), Adrian Perrig (ETH Zurich)

Aliens Among Us: Observing Private or Reserved IPs on the Public Internet
Radu Anghel (TU Delft), Carlos Gañán (ICANN), Qasim Lone (RIPE NCC), Matthew Luckie (CAIDA), Yury Zhauniarovich (TU Delft)

Are your Sites Truly Isolated? Automatically Detecting Logic Bugs in Site Isolation Implementations
Jan Drescher (TU Braunschweig), David Klein (TU Braunschweig), Martin Johns (TU Braunschweig)

Pruning the Tree: Rethinking RPKI Architecture from the Ground up
Haya Schulmann (Goethe-Universität Frankfurt and ATHENE German Research Center for Applied Cybersecurity), Niklas Vogel (Goethe-Universität Frankfurt and ATHENE German Research Center for Applied Cybersecurity)

Session 9A: Fuzzing Shake the Silicon

Fuzzilicon: A Post-Silicon Microcode-Guided x86 CPU Fuzzer
Johannes Lenzen (Technical University of Darmstadt), Mohamadreza Rostami (Technical University of Darmstadt), Lichao Wu (Technical University of Darmstadt), Ahmad-Reza Sadeghi (Technical University of Darmstadt)

GoldenFuzz: Generative Golden Reference Hardware Fuzzing
Lichao Wu (Technical University of Darmstadt), Mohamadreza Rostami (Technical University of Darmstadt), Huimin Li (Technical University of Darmstadt), Nikhilesh Singh (Technical University of Darmstadt), Ahmad-Reza Sadeghi (Technical University of Darmstadt)

ADGFUZZ: Assignment Dependency-Guided Fuzzing for Robotic Vehicles
Yuncheng Wang (Institute of Information Engineering, CAS, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Yaowen Zheng (Institute of Information Engineering, CAS, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Puzhuo Liu (Tsinghua University, China and Ant Group, China), Dongliang Fang (Institute of Information Engineering, CAS, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Jiaxing Cheng (Institute of Information

Engineering, CAS, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Dingyi Shi (Institute of Information Engineering, CAS, China and School of Cyber Security, University of Chinese Academy of Sciences, China), Limin Sun (Institute of Information Engineering, CAS, China and School of Cyber Security, University of Chinese Academy of Sciences, China)

RTCON: Context-Adaptive Function-Level Fuzzing for RTOS Kernels
Eunkyu Lee (KAIST School of Electrical Engineering), Junyoung Park (KAIST School of Electrical Engineering), Insu Yun (KAIST School of Electrical Engineering)

Session 9B: Systems Security The Rise of the Defenders

BINALIGNER: Aligning Binary Code for Cross-Compilation Environment Diffing
Yiran Zhu (The State Key Laboratory of Blockchain and Data Security, Zhejiang University), Tong Tang (The State Key Laboratory of Blockchain and Data Security, Zhejiang University), Jie Wan (The State Key Laboratory of Blockchain and Data Security, Zhejiang University), Ziqi Yang (The State Key Laboratory of Blockchain and Data Security, Zhejiang University; Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security), Zhenguang Liu (The State Key Laboratory of Blockchain and Data Security, Zhejiang University; Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security), Lorenzo Cavallaro (University College London)

Cross-Consensus Reliable Broadcast and its Applications
Yue Huang (Tsinghua University), Xin Wang (Tsinghua University and State Key Laboratory of Cryptography and Digital Economy Security), Haibin Zhang (Yangtze Delta Region Institute of Tsinghua University, Zhejiang), Sisi Duan (Tsinghua University, Zhongguancun Laboratory, Shandong Institute of Blockchains and State Key Laboratory of Cryptography and Digital Economy Security)

vSim: Semantics-Aware Value Extraction for Efficient Binary Code Similarity Analysis
Huaijin Wang (The Ohio State University), Zhiqiang Lin (The Ohio State University)

A Deep Dive into Function Inlining and its Security Implications for ML-based Binary Analysis
Omar Abusabha (Sungkyunkwan University, South Korea), Jiyong Uhm (Sungkyunkwan University, South Korea), Tamer Abuhmed (Sungkyunkwan University, South Korea), Hyungjoon Koo (Sungkyunkwan University, South Korea)

Session 9C: Network Security Silence of the LANs

Time and Time Again: Leveraging TCP Timestamps to Improve Remote Timing Attacks
Vik Vanderlinden (DistriNet, KU Leuven), Tom Van Goethem (DistriNet, KU Leuven), Mathy Vanhoef (DistriNet, KU Leuven)

Continuous User Behavior Monitoring using DNS Cache Timing Attacks
Hannes Weissteiner (Graz University of Technology, Graz, Austria), Roland Czerny (Graz University of Technology, Graz, Austria), Simone Franza (Graz University of Technology, Graz, Austria), Stefan Gast (Graz University of Technology, Graz, Austria), Johanna Ullrich (University of Vienna, Vienna, Austria), Daniel Gruss (Graz University of Technology, Graz, Austria)

On Borrowed Time: Measurement-Informed Understanding of the NTP Pool's Robustness to Monopoly Attacks
Robert Beverly (San Diego State University), Erik Rye (Johns Hopkins University)

Bit of a Close Talker: A Practical Guide to Serverless Cloud Co-Location Attacks
Wei Shao (University of California, Davis), Najmeh Nazari (University of California, Davis), Behnam Omidi (George Mason University), Setareh Rafatirad (University of California, Davis), Khaled N. Khasawneh (George Mason University), Houman Homayoun (University of California Davis), Chongzhou Fang (Rochester Institute of Technology)

Session 9D: Web & Content Security The XSS Files

PANDORA: Lightweight Adversarial Defense for Edge IoT using Uncertainty-Aware Metric Learning
Avinash Awasthi (Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur, India), Pritam Vediya (Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur, India), Hemant Miranka (The LNM Institute of Information Technology, Jaipur, India), Ramesh Babu Battula (Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur, India), Manoj Singh Gaur (Indian Institute of Technology Jammu, Jammu and Kashmir, India)

Strategic Games and Zero Shot Attacks on Heavy-Hitter Network Flow Monitoring
Francesco Da Dalt (ETH Zürich), Adrian Perrig (ETH Zurich)

PhishLang: A Real-Time, Fully Client-Side Phishing Detection Framework Using MobileBERT
Sayak Saha Roy (The University of Texas at Arlington), Shirin Nilizadeh (The University of Texas at Arlington)

CoLD: Collaborative Label Denoising Framework for Network Intrusion Detection
Shuo Yang (The University of Hong Kong, Hong Kong SAR, China), Xinran Zheng (University College London, London, United Kingdom), Jinze Li (The University of Hong Kong, Hong Kong SAR, China), Jinfeng Xu (The University of Hong Kong, Hong Kong SAR, China), Edith C. H. Ngai (TThe University of Hong Kong, Hong Kong SAR, China)

Session 10A: Stealthy Evasion Attacks Seeing Isn't Believing

Targeted Physical Evasion Attacks in the Near-Infrared Domain

Pascal Zimmer (Ruhr University Bochum), Simon Lachnit (Ruhr University Bochum), Alexander Jan Zielinski (Ruhr University Bochum), Ghassan Karame (Ruhr University Bochum)

FlyTrap: Physical Distance-Pulling Attack Towards Camera-based Autonomous Target Tracking Systems

Shaoyuan Xie (University of California, Irvine), Mohamad Habib Fakih (University of California, Irvine), Junchi Lu (University of California, Irvine), Fayzah Alshammari (University of California, Irvine), Ningfei Wang (University of California, Irvine), Takami Sato (University of California, Irvine), Halima Bouzidi (University of California Irvine), Mohammad Abdullah Al Faruque (University of California, Irvine), Qi Alfred Chen (University of California, Irvine)

Understanding the Stealthy BGP Hijacking Risk in the ROV Era

Yihao Chen (DCST & BNRist & State Key Laboratory of Internet Architecture, Tsinghua University; Zhongguancun Laboratory), Qi Li (INSC & State Key Laboratory of Internet Architecture, Tsinghua University; Zhongguancun Laboratory), Ke Xu (DCST & State Key Laboratory of Internet Architecture, Tsinghua University; Zhongguancun Laboratory), Zhuotao Liu (INSC & State Key Laboratory of Internet Architecture, Tsinghua University; Zhongguancun Laboratory), Jianping Wu (INSC & State Key Laboratory of Internet Architecture, Tsinghua University; Zhongguancun Laboratory)

Session 10B: Messaging Security Return of the Phish

TBTrackerX: Fantastic Trigger Bots and Where to Find Malicious Campaigns on X

Mohammad Majid Akhtar (School of Computer Science and Engineering, University of New South Wales, Sydney, Australia), Rahat Masood (School of Computer Science and Engineering, University of New South Wales, Sydney, Australia), Muhammad Ikram (School of Computing, Macquarie University, Sydney, Australia), Salil S. Kanhere (School of Computer Science and Engineering, University of New South Wales, Sydney, Australia)

CoordMail: Exploiting SMTP Timeout and Command Interaction to Coordinate Email Middleware for Convergence Amplification Attack

Ruixuan Li (Tsinghua University and Beijing National Research Center for Information Science and Technology), Chaoyi Lu (Zhongguancun Laboratory), Baojun Liu (Tsinghua University and Beijing National Research Center for Information Science and Technology), Yanzhong Lin (Coremail Technology Co. Ltd), Qingfeng Pan (Coremail Technology Co. Ltd), Jun Shao (Zhejiang Gongshang University and Zhejiang Key Laboratory of Big Data and Future E-Commerce Technology)

One Email, Many Faces: A Deep Dive into Identity Confusion in Email Aliases

Mengying Wu (Fudan University, China), Geng Hong (Fudan University, China), Jiatao Chen (Fudan University, China), Baojun Liu (Tsinghua University, China), Mingxuan Liu (Zhongguancun Laboratory, China), Min Yang (Fudan University, China)

Session 10C: Systems Security Once Upon a Time in Memory

Fast Pointer Nullification for Use-After-Free Prevention
Yubo Du (University of Pittsburgh), Youtao Zhang (University of Pittsburgh), Jun Yang (University of Pittsburgh)

ropbot: Reimaging Code Reuse Attack Synthesis
Kyle Zeng (Arizona State University), Moritz Schloegel (CISPA Helmholtz Center for Information Security), Christopher Salls (UC Santa Barbara), Adam Doupé (Arizona State University), Ruoyu Wang (Arizona State University), Yan Shoshitaishvili (Arizona State University), Tiffany Bao (Arizona State University)

Token Time Bomb: Evaluating JWT Implementations for Vulnerability Discovery
Jingcheng Yang (Tsinghua University), Enze Wang (Tsinghua University and National University of Defense Technology), Jianjun Chen (Tsinghua University), Qi Wang (Tsinghua University), Yuheng Zhang (Tsinghua University), Haixin Duan (Tsinghua University), Wei Xie (National University of Defense Technology), Baosheng Wang (National University of Defense Technology)

Session 11A: Usable Security UX Men: Days of Future Auth

Vault Raider: Stealthy UI-based Attacks Against Password Managers in Desktop Environments
Andrea Infantino (University of Illinois Chicago), Mir Masood Ali (University of Illinois Chicago), Kostas Solomos (University of Illinois Chicago), Jason Polakis (University of Illinois Chicago)

Targeted Password Guessing Using k-Nearest Neighbors
Zhen Li (Nankai University), Ding Wang (Nankai University)

Repairing Trust in Domain Name Disputes Practices: Insights from a Quarter-Century's Worth of Squabbles
Vinny Adjibi (Georgia Institute of Technology), Athanasios Avgetidis (Georgia Institute of Technology), Manos Antonakakis (Georgia Institute of Technology), Alberto Dainotti (Georgia Institute of Technology), Michael Bailey (Georgia Institute of Technology), Fabian Monrose (Georgia Institute of Technology)

Session 11B: Covert Sensing & Privacy Leakage The Walls Have Ears

DualStrike: Accurate, Real-time Eavesdropping and Injection of Keystrokes on Commodity Keyboards
Xiaomeng Chen (Shanghai Jiao Tong University), Jike Wang (Shanghai Jiao Tong University), Zhenyu Chen (Shanghai Jiao Tong University), Qi Alfred Chen (University of California, Irvine), Xinbing Wang (Shanghai Jiao Tong University), Dongyao Chen (Shanghai Jiao Tong University)

Hiding an Ear in Plain Sight: On the Practicality and Implications of Acoustic Eavesdropping with Telecom Fiber Optic Cables
Youqian Zhang (The Hong Kong Polytechnic University), Zheng Fang (The Hong Kong Polytechnic University), Huan Wu (The Hong Kong Polytechnic University & Technological and Higher Education Institute of Hong Kong), Sze Yiu Chau

(The Chinese University of Hong Kong), Chao Lu (The Hong Kong Polytechnic University), Xiapu Luo (The Hong Kong Polytechnic University)

The Role of Privacy Guarantees in Voluntary Donation of Private Health Data for Altruistic Goals

Ruizhe Wang (University of Waterloo), Roberta De Viti (MPI-SWS), Aarushi Dubey (University of Washington), Elissa M. Redmiles (Georgetown University)

Passive Multi-Target GUTI Identification via Visual-RF Correlation in LTE Networks

Byeongdo Hong (The Affiliated Institute of ETRI), Gunwoo Yoon (The Affiliated Institute of ETRI)

Session 11C: Privacy & Measurement Catch Me If You Can, Cookie

Prɛɛmpt: Sanitizing Sensitive Prompts for LLMs

Amrita Roy Chowdhury (University of Michigan, Ann Arbor), David Glukhov (University of Toronto and Vector Institute), Divyam Anshumaan (University of Wisconsin-Madison), Prasad Chalasani (Langroid Incorporated), Nicholas Papernot (University of Toronto and Vector Institute), Somesh Jha (University of Wisconsin-Madison), Mihir Bellare (University of California, San Diego)

PrivORL: Differentially Private Synthetic Dataset for Offline Reinforcement Learning

Chen GONG (University of Virginia), Zheng Liu (University of Virginia), Kecen Li (University of Virginia), Tianhao Wang (University of Virginia)

There is No War in Ba Sing Se: A Global Analysis of Content Moderation in Large Language Models

Friedemann Lipphardt (MPI-INF), Moonis Ali (MPI-INF), Martin Banzer (MPI-INF), Anja Feldmann (MPI-INF), Devashish Gosain (IIT Bombay)

PACS: Privacy-Preserving Attribute-Driven Community Search over Attributed Graphs

Fangyuan Sun (Qingdao University), Yaxi Yang (Singapore University of Technology and Design), Jia Yu (Qingdao University), Jianying Zhou (Singapore University of Technology and Design)

Session 11D: AI & Web Security Mission: Improbable Robustness

Chasing Shadows: Pitfalls in LLM Security Research

Jonathan Evertz (CISPA Helmholtz Center for Information Security), Niklas Risse (Max Planck Institute for Security and Privacy), Nicolai Neuer (Karlsruhe Institute of Technology), Andreas Müller (Ruhr University Bochum), Philipp Normann (TU Wien), Gaetano Sapia (Max Planck Institute for Security and Privacy), Srishti Gupta (Sapienza University of Rome), David Pape (CISPA Helmholtz Center for Information Security), Soumya Shaw (CISPA Helmholtz Center for Information Security), Devansh Srivastav (CISPA Helmholtz Center for Information Security), Christian Wressnegger (Karlsruhe Institute of Technology), Erwin Quiring (_fbeta), Thorsten Eisenhofer (CISPA Helmholtz Center for Information Security), Daniel Arp (TU Wien), Lea Schönherr (CISPA Helmholtz Center for Information Security)

Decompiling the Synergy: An Empirical Study of Human–LLM Teaming in Software Reverse Engineering

Zion Leonahenahe Basque (Arizona State University), Samuele Doria (University of Padua), Ananta Soneji (Arizona State University), Wil Gibbs (Arizona State University), Adam Doupe (Arizona State University), Yan Shoshitaishvili (Arizona State University), Eleonora Losiouk (University of Padua), Ruoyu "Fish" Wang (Arizona State University), Simone Aonzo (EURECOM)

DOM-XSS Detection via Webpage Interaction Fuzzing and URL Component Synthesis

Nuno Sabino (Carnegie Mellon University, Instituto Superior Técnico, Universidade de Lisboa, and Instituto de Telecomunicações), Darion Cassel (Carnegie Mellon University), Rui Abreu (Universidade do Porto, INESC-ID), Pedro Adão (Instituto Superior Técnico, Universidade de Lisboa, and Instituto de Telecomunicações), Lujo Bauer (Carnegie Mellon University), Limin Jia (Carnegie Mellon University)

Small Cell, Big Risk: A Security Assessment of 4G LTE Femtocells in the Wild

Yaru Yang (Tsinghua University), Yiming Zhang (Tsinghua University), Tao Wan (CableLabs & Carleton University), Haixin Duan (Tsinghua University & Quancheng Laboratory), Deliang Chang (QI-ANXIN Technology Research Institute), Yishen Li (Tsinghua University), Shujun Tang (Tsinghua University & QI-ANXIN Technology Research Institute)

Session 12A: Web & Content Security The Phantom of the Opera tor

VICTOR: Dataset Copyright Auditing in Video Recognition Systems

Quan Yuan (Zhejiang University), Zhikun Zhang (Zhejiang University), Linkang Du (Xi'an Jiaotong University), Min Chen (Vrije Universiteit Amsterdam), Mingyang Sun (Peking University), Yunjun Gao (Zhejiang University), Shibo He (Zhejiang University), Jiming Chen (Zhejiang University and Hangzhou Dianzi University)

Revealing The Secret Power: How Algorithms Can Influence Content Visibility on Twitter/X

Alessandro Galeazzi (University of Padua), Pujan Paudel (Boston University), Mauro Conti (University of Padua and Orebro University), Emiliano De Cristofaro (University of California, Riverside), Gianluca Stringhini (Boston University)

CTng: Secure Certificate and Revocation Transparency

Jie Kong (Dept. of Computer Science and Engineering, University of Connecticut, Storrs, CT), Damon James (Dept. of Computer Science and Engineering, University of Connecticut, Storrs, CT), Hemi Leibowitz (Faculty of Computer Science, The College of Management Academic Studies, Rishon LeZion, Israel), Ewa Syta (Dept. of Computer Science, Trinity College, Hartford, CT), Amir Herzberg (Dept. of Computer Science and Engineering, University of Connecticut, Storrs, CT)

Time will Tell: Large-scale De-anonymization of Hidden I2P Services via Live Behavior Alignment

Hongze Wang (Southeast University), Zhen Ling (Southeast University), Xiangyu Xu (Southeast University), Yumingzhi Pan (Southeast University), Guangchi Liu

(Southeast University), Junzhou Luo (Southeast University and Fuyao University of Science and Technology), Xinwen Fu (University of Massachusetts Lowell)

Session 12B: Attacks When Assumptions Fail

BACnet or "BADnet"? On the (In)Security of Implicitly Reserved Fields in BACnet
Qiguang Zhang (Southeast University), Junzhou Luo (Southeast University, Fuyao University of Science and Technology), Zhen Ling (Southeast University), Yue Zhang (Shandong University), Chongqing Lei (Southeast University), Christopher Morales (University of Massachusetts Lowell), Xinwen Fu (University of Massachusetts Lowell)

Scalable Off-Chain Auctions
Mohsen Minaei (Visa Research), Ranjit Kumaresan (Visa Research), Andrew Beams (Visa Research), Pedro Moreno-Sanchez (IMDEA Software Institute, MPI-SP), Yibin Yang (Georgia Institute of Technology), Srinivasan Raghuraman (Visa Research and MIT), Panagiotis Chatzigiannis (Visa Research), Mahdi Zamani (Visa Research), Duc V. Le (Visa Research)

LOKI: Proactively Discovering Online Scam Websites by Mining Toxic Search Queries
Pujan Paudel (Boston University), Gianluca Stringhini (Boston University)

QNBAD: Quantum Noise-induced Backdoor Attacks against Zero Noise Extrapolation
Cheng Chu (Indiana University Bloomington), Qian Lou (University of Central Florida), Fan Chen (Indiana University Bloomington), Lei Jiang (Indiana University Bloomington)

Session 12C: Connectivity & Privacy Plug, Play, and Pray

WCDCAnalyzer: Scalable Security Analysis of Wi-Fi Certified Device Connectivity Protocols
Zilin Shen (Purdue University), Imtiaz Karim (The University of Texas at Dallas), Elisa Bertino (Purdue University)

PriSrv+: Privacy and Usability-Enhanced Wireless Service Discovery with Fast and Expressive Matchmaking Encryption
Yang Yang (Singapore Management University), Guomin Yang (Singapore Management University), Yingjiu Li (University of Oregon, USA), Pengfei Wu (Singapore Management University), Rui Shi (Hainan University, China), Minming Huang (Singapore Management University), Jian Weng (Jinan University, Guangzhou, China), HweeHwa Pang (Singapore Management University), Robert H. Deng (Singapore Management University)

Mapping the Cloud: A Mixed-Methods Study of Cloud Security and Privacy Configuration Challenges
Sumair Ijaz Hashmi (CISPA Helmholtz Center for Information Security, Germany, Saarland University, Germany and Lahore University of Management Sciences (LUMS), Pakistan), Shafay Kashif (The University of Auckland, New Zealand and Lahore University of Management Sciences (LUMS), Pakistan), Lea Gröber (International Computer Science Institute (ICSI), USA and Lahore University of Management Sciences (LUMS), Pakistan), Katharina Krombholz (CISPA

Helmholtz Center for Information Security, Germany), Mobin Javed (Lahore University of Management Sciences (LUMS), Pakistan)

To Shuffle or not to Shuffle: Auditing DP-SGD with Shuffling
Meenatchi Sundaram Muthu Selva Annamalai (University College London), Borja Balle (Google Deepmind), Jamie Hayes (Deepmind), Emiliano De Cristofaro (University of California, Riverside)

Session 13A: Applied Cryptography

Icarus: Achieving Performant Asynchronous BFT with Only Optimistic Paths
Xiaohai Dai (Huazhong University of Science and Technology), Yiming Yu (Huazhong University of Science and Technology), Sisi Duan (Tsinghua University), Rui Hao (Wuhan University of Technology), Jiang Xiao (Huazhong University of Science and Technology), Hai Jin (Huazhong University of Science and Technology)

SoK: Cryptographic Authenticated Dictionaries
Harjasleen Malvai (University of Illinois, Urbana-Champaign), Francesca Falzon (ETH Zürich), Andrew Zitek-Estrada (EPFL), Sarah Meiklejohn (University College London), Joseph Bonneau (NYU)

Action Required: A Mixed-Methods Study of Security Practices in GitHub Actions
Yusuke Kubo (NTT DOCOMO BUSINESS, Inc. / Waseda University), Fumihiro Kanei (NTT DOCOMO BUSINESS, Inc.), Mitsuaki Akiyama (NTT, Inc.), Takuro Wakai (Waseda University), Tatsuya Mori (Waseda University / NICT / RIKEN AIP)

Analysis of the Security Design, Engineering, and Implementation of the SecureDNA System
Alan T. Sherman (University of Maryland, Baltimore County (UMBC)), Jeremy J. Romanik Romano (University of Maryland, Baltimore County (UMBC)), Edward Zieglar (University of Maryland, Baltimore County (UMBC)), Enis Golaszewski (University of Maryland, Baltimore County (UMBC)), Jonathan D. Fuchs (University of Maryland, Baltimore County (UMBC)), William E. Byrd (University of Alabama at Birmingham)

Session 13B: Network Security Game of Flows

PathProb: Probabilistic Inference and Path Scoring for Enhanced and Flexible BGP Route Leak Detection
Yingqian Hao (Computer Network Information Center, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Hui Zou (Computer Network Information Center, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Lu Zhou (Computer Network Information Center, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Yuxuan Chen (Computer Network Information Center, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Yanbiao Li (Computer Network Information Center, Chinese Academy of Sciences; University of Chinese Academy of Sciences)

Demystifying RPKI-Invalid Prefixes: Hidden Causes and Security Risks
Weitong Li (Virginia Tech), Tao Wan (CableLabs), Tijay Chung (Virginia Tech)

Know Me by My Pulse: Toward Practical Continuous Authentication on Wearable Devices via Wrist-Worn PPG
Wei Shao (University of California, Davis), Zequan Liang (University of California Davis), Ruoyu Zhang (University of California, Davis), Ruijie Fang (University of California, Davis), Ning Miao (University of California, Davis), Ehsan Kourkchi (University of California - Davis), Setareh Rafatirad (University of California, Davis), Houman Homayoun (University of California Davis), Chongzhou Fang (Rochester Institute of Technology)

The Heat is On: Understanding and Mitigating Vulnerabilities of Thermal Image Perception in Autonomous Systems
Sri Hrushikesh Varma Bhupathiraju (University of Florida), Shaoyuan Xie (University of California, Irvine), Michael Clifford (Toyota InfoTech Labs), Qi Alfred Chen (University of California, Irvine), Takeshi Sugawara (The University of Electro-Communications), Sara Rampazzi (University of Florida)

Session 13C: Cloud Security Death by a Thousand Abstractions

The Dark Side of Flexibility: Detecting Risky Permission Chaining Attacks in Serverless Applications
Xunqi Liu (State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University), Nanzi Yang (University of Minnesota), Chang Li (State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University), Jinku Li (State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University), Jianfeng Ma (State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University), Kangjie Lu (University of Minnesota)

Breaking the Bulkhead: Demystifying Cross-Namespace Reference Vulnerabilities in Kubernetes Operators
Andong Chen (Zhejiang University), Ziyi Guo (Northwestern University), Zhaoxuan Jin (Northwestern University), Zhenyuan Li (Zhejiang University), Yan Chen (Northwestern University)

SIPConfusion: Exploiting SIP Semantic Ambiguities for Caller ID and SMS Spoofing
Qi Wang (Tsinghua University), Jianjun Chen (Tsinghua University), Jingcheng Yang (Tsinghua University), Jiahe Zhang (Tsinghua University), Yaru Yang (Tsinghua University), Haixin Duan (Tsinghua University)

Looma: A Low-Latency PQTLS Authentication Architecture for Cloud Applications
Xinshu Ma (University of Edinburgh), Michio Honda (University of Edinburgh)

Session 13D: Malware & Reverse Engineering Reverse, Reverse

Unveiling BYOVD Threats: Malware's Use and Abuse of Kernel Drivers
Andrea Monzani (University of Milan), Antonio Parata (University of Milan), Andrea Oliveri (EURECOM), Simone Aonzo (EURECOM), Davide Balzarotti (EURECOM), Andrea Lanzi (University of Milan)

Understanding the Status and Strategies of the Code Signing Abuse Ecosystem
Hanqing Zhao (Tsinghua University & QI-ANXIN Technology Research Institute), Yiming Zhang (Tsinghua University), Lingyun Ying (QI-ANXIN Technology Research Institute), Mingming Zhang (Zhongguancun Laboratory), Baojun Liu (Tsinghua University), Haixin Duan (Tsinghua University), Zi-Quan You (Tsinghua University), Shuhao Zhang (QI-ANXIN Technology Research Institute)

SYSYPHUZZ: the Pressure of More Coverage
Zezhong Ren (University of Chinese Academy of Sciences; EPFL), Han Zheng (EPFL), Zhiyao Feng (EPFL), Qinying Wang (EPFL), Marcel Busch (EPFL), Yuqing Zhang (University of Chinese Academy of Sciences), Chao Zhang (Tsinghua University), Mathias Payer (EPFL)

Actively Understanding the Dynamics and Risks of the Threat Intelligence Ecosystem
Tillson Galloway (Georgia Institute of Technology), Omar Alrawi (Georgia Institute of Technology), Allen Chang (Georgia Institute of Technology), Athanasios Avgetidis (Georgia Institute of Technology), Manos Antonakakis (Georgia Institute of Technology), Fabian Monrose (Georgia Institute of Technology)

Message from the General Chairs

Welcome to the 2026 Network and Distributed System Security (NDSS) Symposium!

This year, the organizing and technical program committees have put together an exceptional program featuring 265 papers, two distinguished keynotes—Dan Wallach, Program Manager at DARPA/I2O, and William Enck, Professor at North Carolina State University—along with a poster session showcasing 41 posters and ten 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, Hamed Okhravi and Ivan Martinovic, for curating an outstanding technical program. NDSS 2026 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 Mathy Vanhoef and Daniele Antonioli for leading the artifact evaluation initiative, which evaluated 114 artifacts. We also extend 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 Sébastien Bardin and Christophe Hauser for organizing an impressive set of co-located events this year, including:

1. Security and Privacy of Next-Generation Networks (FutureG)
2. Attack Provenance, Reasoning, and Investigation for Security in the Monitored Environment (PRISM)
3. Security and Privacy in Standardized IoT (SDIoTSec)
4. Security of Space and Satellite Systems (SpaceSec)
5. SOC Operations and Construction (WOSOC)
6. Binary Analysis Research (BAR)
7. Fuzzing Workshop (FUZZING)
8. LLM Assisted Security and Trust Exploitation (LAST-X)
9. Measurements, Attacks, and Defenses for the Web (MADWeb)
10. Usable Security and Privacy (USEC)

We also extend our thanks to Kaushal Kafle and Muslum Ozgur Ozmen for coordinating a fantastic poster session, and for organizing the Best Poster Awards. Special appreciation goes to Dan Lin and her team for reviewing student fellowship applications—this year, 20 students received NDSS fellowships and travel support.

Further thanks to Yue Xiao, our publicity 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 Sponsors TikTok and Ericsson; Silver Sponsors Ant Group, Google, FutureWei Technologies, and Palo Alto Networks; Bronze Sponsor Qualcomm; and our lanyard sponsor CISPA. Palo Alto Networks also sponsored Best Paper awards for the MADWeb and PRISM workshops.

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 2026!

Heng Yin and Mauro Conti
General Chairs, NDSS 2026

Message from the Program Committee Co-Chairs

We are pleased to present the technical program of the 2026 Network and Distributed System Security (NDSS) Symposium, held in person from February 23 to 28, 2026. Now in its 34th edition and organized by the Internet Society (ISOC) since its inception, NDSS has established itself as a ptop-tier venue for cybersecurity research, with a particular focus on network and systems security. The symposium emphasizes practical, impactful solutions, making it highly relevant to both academia and industry.

Cybersecurity continues to evolve rapidly, reflected in the strong engagement from the research community this year. A total of 1,481 submissions entered the review process across two submission cycles, excluding papers that were out of scope or did not meet submission guidelines. Submissions were evaluated based on technical quality, novelty, and significance. Each cycle involved two rounds of review, with additional reviews when necessary, and oversight by the Ethics Review Board where applicable. Papers receiving two clearly negative reviews were rejected after the first round, while the remainder advanced to the second round. Most papers in the second round received four or more reviews, with others receiving at least three.

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.

We worked to ensure that the review process was both rigorous and constructive. Authors benefited from a rebuttal phase and interactive discussions, and Program Committee (PC) members were encouraged to highlight strengths and provide actionable feedback. In total, 265 papers were accepted to the program, corresponding to an acceptance rate of 17.89%. Among these, 142 papers were accepted after major revisions. Of the accepted papers, 114 submitted artifacts for evaluation; 112, 97, and 70 received the Available, Functional, and Reproduced badges, respectively.

This year, we placed particular emphasis on improving the scalability, integrity, and ethical rigor of the review process, as well as addressing the growing role of generative AI. To support these goals, we introduced five key initiatives: humane reviewing practices (ensuring that the review process allows sufficient time while avoiding deadlines on weekends and major holidays), the introduction of the role of Associate Chair, expansion of specialized subcommittees (for ethics, awards, and topic vetting), a submission cap of six papers per cycle, and an optional presentation model.

We extend our sincere thanks to the Associate Chairs (Amir Houmansadr, Aravind Machiry, Awais Rashid, Brendan Saltaformaggio, Ghassan Karame, Kevin Butler, Nader Sehatbakhsh, Nathan Burow, Selcuk Uluagac, and William Robertson), whose professionalism was instrumental in maintaining the highest standards of the review process. We are also deeply grateful to the PC members and external reviewers. Serving on the PC required significant commitment: 274 experts joined the NDSS ’26 Technical Program Committee, 204 of whom participated in both cycles. PC members contributed up to 10 reviews in the Summer cycle and up to 12 in the Fall cycle, in addition to engaging in discussions, interacting with authors, and serving as shepherds or discussion leads. NDSS would not be possible without their dedication.

We also thank the Artifact Evaluation Committee for their careful assessments, as well as the members of the Ethics Review Board, Topic Concern Subcommittee, and Best Paper Award Subcommittee for their essential contributions.

Organizing a conference of this scale is a substantial effort, and we are grateful to all who contributed. We would like to highlight a few individuals in particular. Heng Yin and Mauro Conti, as Organization Committee Chairs, provided invaluable guidance throughout the process. Steering Committee Chair Yongdae Kim offered critical oversight and support on key decisions. Robin Wilton played a vital coordinating role across the Program Committee, Organizing Committee, and ISOC. From ISOC and AMS, Ivana Trbovic, Jennifer Higgins, and Gabby Croghan provided excellent operational support. Artifact Evaluation Co-Chairs Mathy Vanhoef and Daniele Antonioli led the artifact evaluation process with exceptional care, reinforcing its importance within NDSS. Finally, Mridula Singh and Hyungsub Kim expertly managed the production of the proceedings. It has been a privilege 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 for joining us online; we are sorry you could not make it in person for reasons beyond your control.

We thank all authors who submitted their work to NDSS 2026 and all attendees joining us in person. We also acknowledge those authors who opted not to present and regret that they could not attend.

We hope you enjoy the conference!

Hamed Okhravi and Ivan Martinovic
Program Committee Co-Chairs, NDSS 2026

Message from the Internet Society

The Internet Society is once again delighted to host the Network and Distributed System Security (NDSS) Symposium in 2026, continuing our decades-long commitment to research at the leading edge of cybersecurity. Thanks to the breadth and quality of your research, the Symposium remains in the top three global cybersecurity conferences. The leadership you demonstrate in your fields of study supports the Internet Society in its mission of creating an Internet that is open, globally-connected, secure, and trustworthy, for everyone. Thank you.

For NDSS, 2026 was yet another year of new records. Paper submissions increased yet again, from around 1300 last year to almost 1600 this year. The Committee Chairs responded with dedication and creativity, recruiting over 260 reviewers and introducing a new layer of 10 Associate Chairs, to turn all those papers into this week's coherent and compelling program.

With so many submissions, a 3-day Symposium would not have been long enough, even with the four tracks we now have. Therefore, for the first time, the Committees offered the option of having papers included in the proceedings without presentation. As a result, we have 265 accepted papers, of which almost 200 will be presented. This year we will also run a record 10 full-day workshops, on the Monday and Friday of NDSS week, which means that the full proceedings for NDSS 2026 will be well over 300 papers.

As ever, with an acceptance rate of under 17%, competition to present at NDSS 2026 was fierce: congratulations to the researchers who will showcase their work at the symposium. This is an incredible achievement, and we at the Internet Society are already working to curate your research, publicize it to a global audience, and use it in our advocacy work for a secure, trustworthy Internet.

None of this could happen without the hard work of General Co-Chairs Heng Yin and Mauro Conti, Program Committee Co-Chairs Hamed Okhravi and Ivan Martinovic, 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 help us develop the student support program into a fully-fledged Internet Society NDSS Fellowship. This is volunteer effort on a massive scale, and we recognize and applaud everyone who contributes, year on year.

In addition to welcoming this year's two symposium keynote speakers, Prof. Dan Wallach (DARPA) and Prof. William Enck (North Carolina State University), we also want to commend Stephen Smalley and Robert Craig, whose 2013 paper on mandatory access control (MAC) for Android won the NDSS Symposium's Test of Time award for 2026. There are few better indicators of the quality of NDSS research than to see one of its papers still shaping the cybersecurity world, over a decade after publication.

Finally, I want to thank all the sponsors without whom this event would not be possible.

This includes our Gold Sponsors TikTok and Ericsson; Silver Sponsors Ant Group, Google, FutureWei and Palo Alto Networks; Bronze Sponsor Qualcomm; and our Lanyard Sponsor CISPA. Palo Alto Networks have also kindly sponsored Best Paper awards for MADWeb, and for a workshop making its debut at NDSS this year, PRISM.

Please make the most of your time here with us at NDSS: learn, network, socialize and develop. But above all, enjoy this opportunity to spend time with like-minded researchers from across the world. NDSS is a global conference: when we talk to each other and exchange ideas, it benefits us all.

Sally Wentworth
President and CEO, Internet Society

Program Committee

Hamed Okhravi, *MIT Lincoln Laboratory* (Co-Chair)
Ivan Martinovic, *University of Oxford* (Co-Chair)

Adam Bates, *University of Illinois at Urbana-Champaign*
Adithya Vadapalli, *IIT Kanpur*
Adwait Nadkarni, *William & Mary*
Afsah Anwar, *University of New Mexico*
Aggelos Kiayias, *University of Edinburgh and IOG*
Ahmad-Reza Sadeghi, *TU Darmstadt*
Aisha Ali-Gombe, *Louisiana State University*
Alessandro Sorniotti, *IBM Research Europe*
Alessio Merlo, *CASD – School of Advanced Defense Studies*
Alexandra Dmitrienko, *University of Wuerzburg*
Alsharif Abuadbba, *CSIRO's Data61*
Alvaro Cardenas, *University of California, Santa Cruz*
Amin Kharraz, *Florida International University*
Amin Sakzad, *Monash University*
Amir Herzberg, *University of Connecticut*
Amir Rahmati, *Stony Brook University*
Amit Klein, *Hebrew University of Jerusalem*
Anat Bremler-Barr, *Tel-Aviv University*
Andrea Mambretti, *IBM Research Europe – Zurich*
Ang Li, *The University of Michigan-Dearborn*
Angelos Stavrou, *Virginia Tech*
Anindya Maiti, *University of Oklahoma*
Anrin Chakraborti, *University of Illinois at Chicago*
Ante Derek, *University of Zagreb*
Antonino Nocera, *University of Pavia*
Anupam Das, *North Carolina State University*
Arash Shaghaghi, *The University of New South Wales (UNSW Sydney)*
Arkady Yerukhimovich, *George Washington University*
Arslan Khan, *Pennsylvania State University*
Arthur Gervais, *University College London (UCL) & Berkeley RDI*
Ashraf Matrawy, *Carleton University*
Azadeh Tabiban, *University of Manitoba*
Bart Coppens, *Ghent University*
Berk Gulmezoglu, *Iowa State University*
Bhavani Thuraisingham, *The University of Texas at Dallas*
Binbin Zhao, *Zhejiang University*
Binghui Wang, *Illinois Institute of Technology*
Bo Luo, *University of Kansas*

Brad Reaves, *NC State*
Cameron Morris, *MITRE*
Carlo Mazzocca, *University of Salerno*
Charalampos Papamanthou, *Yale University*
Chenglin Miao, *Iowa State University*
Chenxiong Qian, *The University of Hong Kong*
Chongzhou Fang, *Rochester Institute of Technology*
Christian Wressnegger, *Karlsruhe Institute of Technology*
Christina Pöpper, *New York University Abu Dhabi*
Christine Utz, *Radboud University*
Christophe Hauser, *Dartmouth College*
Christopher Kruegel, *UC Santa Barbara*
Coby Wang, *Visa Research*
Cong Sun, *Xidian University*
Daisuke Mashima, *Singapore University of Technology and Design*
Daniel Gruss, *Graz University of Technology*
Daniele Cono D'Elia, *Sapienza University of Rome*
Daoyuan Wu, *Lingnan University, Hong Kong*
Dean Sullivan, *University of New Hampshire*
Debin Gao, *Singapore Management University*
Derrick McKee, *MIT Lincoln Laboratory*
Derui Wang, *CSIRO's Data61*
Doowon Kim, *University of Tennessee, Knoxville*
Eduard Marin, *Telefonica Research*
Eleonora Losiouk, *University of Padua*
Elias Athanasopoulos, *University of Cyprus*
Elizabeth A. Quaglia, *Royal Holloway, University of London*
Emil Lupu, *Imperial College London*
Engin Kirda, *Northeastern University*
Eric Wustrow, *University of Colorado Boulder*
Erik van der Kouwe, *Vrije Universiteit Amsterdam*
Eugene Vasserman, *Kansas State University*
Euijin Choo, *University of Alberta*
Evgenios Kornaropoulos, *George Mason University*
Farinaz Koushanfar, *UCSD*
Faysal Hossain Shezan, *University of Texas at Arlington*
Fengwei Zhang, *Southern University of Science and Technology*
Filipo Sharevski, *DePaul University*
Flavio Toffalini, *Ruhr University Bochum*
Gabriele Oligeri, *Hamad Bin Khalifa University*
Gail-Joon Ahn, *Arizona State University*
Gang Qu, *University of Maryland, College Park*
Gaoning Pan, *Hangzhou Dianzi University*

Gaurav Panwar, *New Mexico State University*
George Danezis, *University College London (UCL)*
Guenevere Chen, *UT San Antonio*
Guofei Gu, *Texas A&M University*
Guohao Lan, *Delft University of Technology*
Guoxing Chen, *Shanghai Jiao Tong University*
Habiba Farrukh, *University of California, Irvine*
Haipeng Cai, *University at Buffalo, SUNY*
Hamed Haddadi, *Imperial College London & Brave Software*
Hamed Nemati, *KTH Royal Institute of Technology*
Han Qiu, *Tsinghua University*
Hang Zhang, *Indiana University*
Hanqing Guo, *University of Hawaii at Manoa*
Haojin Zhu, *Shanghai Jiao Tong University*
Harshad Sathaye, *ETH Zurich*
Hong Hu, *The Pennsylvania State University*
Hossein Fereidooni, *KOBIL GmbH*
Hossein Yalame, *Bosch Research*
Houman Homayoun, *University of California Davis*
Hyungsub Kim, *Indiana University Bloomington*
Imtiaz Karim, *The University of Texas at Dallas*
Insu Yun, *KAIST*
Jeyavijayan Rajendran, *TAMU*
Jianjun Chen, *Tsinghua University*
Johanna Ullrich, *SBA Research/Universität Wien*
Johannes Kinder, *LMU Munich*
John Criswell, *University of Rochester*
Junghwan Rhee, *University of Central Oklahoma*
Kai Li, *San Diego State University*
Kaihua Qin, *Yale University*
Kangjie Lu, *University of Minnesota*
Kapil Singh, *IBM T.J. Watson Research Center*
Karthika Subramani, *Georgia Tech*
Kasper Rasmussen, *University of Oxford*
Katsunari Yoshioka, *Yokohama National University*
Kaushal Kafle, *University of South Florida*
Kevin Borgolte, *Ruhr University Bochum*
Kevin Hamlen, *UT Dallas*
Kevin Leach, *Vanderbilt University*
Khaled N. Khasawneh, *George Mason University*
Kun Sun, *George Mason University*
Kyu Hyung Lee, *University of Georgia*
Lannan Lisa Luo, *George Mason University*

Le Guan, *University of Georgia*
Lejla Batina, *Radboud University*
Lichao Wu, *TU Darmstadt*
Lingyu Wang, *University of British Columbia (Okanagan Campus)*
Lucas Davi, *University of Duisburg-Essen*
Luyi Xing, *University of Illinois Urbana-Champaign/Indiana University Bloomington*
Man-Ki Yoon, *North Carolina State University*
Manuel Egele, *Boston University*
Marco Balduzzi, *Trend Micro Research*
Marcus Botacin, *Texas A&M University*
Marcus Peinado, *Microsoft Research*
Martin Henze, *RWTH Aachen University & Fraunhofer FKIE*
Martin Johns, *TU Braunschweig*
Martin Strohmeier, *Cyber-Defence Campus, armasuisse Science + Technology*
Martina Lindorfer, TU Wien
Matteo Grosse-Kampmann, *Rhine-Waal University / AWARE7 GmbH*
Meng Luo, *Zhejiang University*
Mengyuan Li, *USC*
Michael Schwarz, *CISPA Helmholtz Center for Information Security*
Michael Specter, *Georgia Tech*
Michael Waidner, *ATHENE National Research Center for Applied Cybersecurity*
Michail Maniatakos, *New York University Abu Dhabi*
Min Suk Kang, *KAIST*
Ming Li, *University of Texas at Arlington*
Ming Xu, *National University of Singapore*
Minghong Fang, *University of Louisville*
Mitsuaki Akiyama, *NTT*
Mohammad Mannan, *Concordia University*
Mridula Singh, *CISPA Helmholtz Center for Information Security*
Muhammad Ikram, *Macquarie University*
Muhammad Lutfor Rahman, *California State University San Marcos*
Murtuza Jadliwala, *The University of Texas at San Antonio*
Muslum Ozgur Ozmen, *Arizona State University*
Neil Gong, *Duke University*
Nikhilesh Singh, *TU Darmstadt*
Nikolaos Alexopoulos, *Athens University of Economics and Business*
Ning Wang, *University of South Florida*
Ning Zhang, *Washington University in St. Louis*
Ningfei Wang, *Independent Researcher*
Ningyu He, *The Hong Kong Polytechnic University*
Norrathep Rattanavipanon, *Prince of Songkla University*
Oleksii Starov, *Palo Alto Networks*
Omar Alrawi, *Georgia Tech*

Omid Mirzaei, *Cisco Talos*
Panagiotis Andriotis, *University of Birmingham*
Panos Papadimitratos, *KTH Royal Institute of Technology*
Paria Shirani, *University of Ottawa*
Pascal Cotret, *Lab-STICC / ENSTA Bretagne*
Peng Gao, *Virginia Tech*
Pubali Datta, *University of Massachusetts Amherst*
Qi Li, *Tsinghua University*
Qian Lou, *University of Central Florida*
Qiben Yan, *Michigan State University*
Qin Wang, *CSIRO Data61*
Rahul Chatterjee, *University of Wisconsin-Madison*
Rajvardhan Oak, *University of California Davis*
Reham Aburas, *American University of Sharjah*
Reza Tourani, *Saint Louis University*
Robert Cunningham, *University of Pittsburgh*
Rui Tan, *Nanyang Technological University*
Ruimin Sun, *Florida International University*
Ruoyu “Fish” Wang, *Arizona State University*
Ryan Kastner, *UCSD*
Sadegh Torabi, *George Mason University*
Saman Zonouz, *Georgia Institute of Technology*
Samuel Jero, *MIT Lincoln Laboratory*
Samuel Mergendahl, *MIT Lincoln Laboratory*
Sanchari Das, *University of Denver*
Sanchuan Chen, *Ohio State University*
Savio Sciancalepore, *TU Eindhoven (TU/e)*
Sebastian Kohler, *University of Oxford*
Sebastien Bardin, *CEA List, University Paris Saclay*
Seongil WI, *UNIST*
Sepideh Ghanavati, *University of Maine*
Shagufta Mehnaz, *Pennsylvania State University*
Shahin Tajik, *Worcester Polytechnic Institute*
Shih-Wei Li, *National Taiwan University*
Shirin Nilizadeh, *The University of Texas at Arlington*
Shu Wang, *Palo Alto Networks, Inc.*
Shuai Hao, *Old Dominion University*
Shweta Shinde, *ETH Zurich*
Simon Birnbach, *University of Oxford*
Sisi Duan, *Tsinghua University*
Soheil Salehi, *The University of Arizona*
Song Fang, *University of Oklahoma*
Song Liao, *Texas Tech University*

Sooel Son, *KAIST*
Srdjan Capkun, *ETH Zurich*
Stefan Katzenbeisser, *Passau University*
Stefan Mangard, *Graz University of Technology*
Stefan Nagy, *University of Utah*
Stefano Zanero, *Politecnico di Milano*
Steven Murdoch, *University College London*
Stjepan Picek, *Radboud University*
Suryadipta Majumdar, *Concordia University*
Syed Rafiul Hussain*, Pennsylvania State University*
Taegyu Kim, *Pennsylvania State University*
Takayuki Sasaki, *Yokohama National University*
Takuya Watanabe, *Deloitte Tohmatsu Cyber LLC*
Tao Ni, *City University of Hong Kong*
Theodor Schnitzler, *Maastricht University*
Thorsten Holz, *Max Planck Institute for Security and Privacy*
Tianwei Zhang, *Nanyang Technological University*
Tiffany Bao, *Arizona State University*
Tim Leek, *MIT Lincoln Laboratory*
Ting Wang, *Stony Brook University*
Tom Chothia, *University of Birmingham*
Tommaso Innocenti, *AWS Amazon*
Torsten Krauß, *University of Würzburg*
Vasudev Gohil, *Siemens EDA*
Veelasha Moonsamy, *Ruhr University Bochum*
Vincent Cheval, *University of Oxford*
Vincent Lenders, *University of Luxembourg*
Wajih Ul Hassan, *University of Virginia*
Wenke Lee, *Georgia Institute of Technology*
William Stephenson, *MIT Lincoln Laboratory*
Xiangkun Jia, *Institute of Software Chinese Academy of Sciences*
Xiaokuan Zhang, *George Mason University*
Xinwen Fu, *University of Massachusetts Lowell*
Xueqiang Wang, *University of Central Florida*
Yan Chen, *Northwestern University*
Yang Xiao, *University of Kentucky*
Yimin Chen, *University of Massachusetts Lowell*
Yinzhi Cao, *Johns Hopkins University*
Yongdae Kim, *KAIST*
Yuan Hong, *University of Connecticut*
Yuan Xiao, *ShanghaiTech University*
Yue Zhang, *Drexel University*
Yunsi Fei, *Northeastern University*

Yuseok Jeon, *Korea University*
Yuzhe Tang, *Syracuse University*
Z. Berkay Celik, *Purdue University*
Zephyr Yao, *New Jersey Institute of Technology*
Zhemin Yang, *Fudan University*
Zhou Li, *University of California, Irvine*
Zhuoqing Mao, *University of Michigan*
Zihao Zhan, *Texas Tech University*
Ziming Zhao, *Northeastern University*
Zitao Chen, *University of Kansas*

External Reviewers

Aleksandr Nahapetyan, *NC State University*
Ali Pourghasemi Fatideh, *University of Maine*
Alireza Famili, *WaveWave Inc.*
Andrea Lin, *MIT Lincoln Laboratory*
Arash Daneshmand, *The University of British Columbia (Okanagan Campus)*
Beomseok Oh, *KAIST*
Bergen Davis, *Concordia University*
Chenang Li, *UC Irvine*
Clark LaChance, *University of Maine*
Cuifeng Gao, *Lingnan University*
Daniel Timko, *SmishTank.com*
David Adei, *NC State University*
Di Wu, *George Mason University*
Dohyun Kim, *KAIST*
Hengkai Ye, *Pennsylvania State University*
Hinddeep Purohit, *Concordia University*
Hugo Kermabon-Bobinnec, *Concordia University*
Ifteher Alom, *University of Kentucky*
Ildi Alla, *University of Luxembourg*
J. Parker Diamond, *MIT Lincoln Laboratory*
Jaehoon Kim, *KAIST*
Jan Drescher, *TU Braunschweig*
Jiaqin Yan, *Shanghai Jiao Tong University*
Jingzhou Ye, *University of Central Florida*
Jiwoo Suh, *KAIST*
Juantao Zhong, *Lingnan University*
Juliana Furgala, *MIT Lincoln Laboratory*
Luis Burbano, *University of California, Santa Cruz*
Lukas Maar, *Graz University of Technology*
Malte Wessels, *TU Braunschweig*
Manuel Karl, *TU Braunschweig*
Minsun Shim, *UC Irvine*
Nicholas Miazzo, *University of Padua*
Peiyang Li, *Tsinghua University*
Qianhui Dai*, Shanghai Jiao Tong University*
Robin Kirchner, *TU Braunschweig*
Ruibo Lu, *Pennsylvania State University*
Samuele Doria, *University of Padua*
Sangmin Woo, *KAIST*
Sara Haghighi, *University of Maine*
Sareh Mohammadi, *Concordia University*
Sergio Valderrama, *University of California, Santa Cruz*

Shadi Babaei, *University of Maine*
Shiqi Liu, *George Mason University*
Shuangpeng Bai, *Pennsylvania State University*
Sotiris Michaelides, *RWTH Aachen University*
Stefan Lenz, *RWTH Aachen University*
Tolga Atalay, *A2Labs LLC*
Tuan Dinh Hoang, *KAIST*
Vijayanta Jain, *University of Maine*
Wei-Cheng Wu, *Dartmouth College*
Wenxin Luo, *Lingnan University*
Xinhao Deng, *Tsinghua University*
Xiyuan Zhao, *Tsinghua University*
Xuesong Bai, *UC Irvine*
Ye Wang, *Tsinghua University*
Yixuan Yang, *Lingnan University*
Yu Zheng, *UC Berkeley*
Yunpeng Liu, *Tsinghua University*
Yuqi Qing, *Tsinghua University*
Zhechang Zhang, *Pennsylvania State University*
Zhen Huang, *Shanghai Jiao Tong University*

Artifact Evaluation Committee

Mathy Vanhoef, *KU Leuven* (Co-Chair)
Daniele Antonioli, *EURECOM* (Co-Chair)

Abdullah Al Ishtiaq, *The Pennsylvania State University*
Alessandro Erba, *Karlsruhe Institute of Technology*
Ali Ranjbar, *The Pennsylvania State University*
Amit Samanta, *University of Utah*
Andrew Roberts, *KTH Sweden*
Angelos Bietis, *DistriNet, KU Leuven*
Arman Riasi, *Virginia Tech*
Ayushi Sharma, *Purdue University*
Boheng Li, *Nanyang Technological University*
Cen Zhang, *Georgia Institute of Technology*
Chakshu Gupta, *University of Twente*
Changming Liu, *Google*
Chaoqi Zhang, *Indiana University Bloomington*
Christian van Sloun, *RWTH Aachen University*
Christoph Sendner, *University of California, Irvine*
Chuanpu Fu, *Tsinghua University*
Chuanqi Xu, *Yale University*
Corban Villa, *UC Berkeley*
Cristian Assaiante, *Sapienza University of Rome*
Denis Donadel, *University of Verona*
Diksha Goel, *CSIRO's Data61, Australia*
Dipsy Desai, *University of Southern California*
Dominik Roy George, *Eindhoven University of Technology*
Enrico Bassetti, *European Space Agency, TU Delft*
Eric Ackermann, *CISPA*
Evangelos Bitsikas, *Northeastern University*
Fabian Bäumer, *Ruhr University Bochum*
Fabian Fleischer, *Georgia Institute of Technology*
Felix Lange, *Paderborn University*
Fuman Xie, *The University of Queensland*
Georgio Nicolas, *COSIC, KU Leuven*
Giorgia Di Pietro, *Sapienza University of Rome*
Gregor Haywood, *Abertay University*
Grigoris Ntousakis, *Brown University*
Guangjing Wang, *University of South Florida*
Halima Bouzidi, *University of California, Irvine*
Haobin Hiroki Chen, *Indiana University Bloomington*
Heloise Gollier, *DistriNet, KU Leuven*

Hengkai Ye, *The Penn State University*
Hongsheng Hu, *University of Newcastle*
Hongyan Chang, *Mohamed bin Zayed University of Artificial Intelligence*
Huaien Zhang, *The University of Hong Kong*
Hung-Mao Chen, *George Mason University*
Jacob Ginesin, *Northeastern University / Carnegie Mellon University*
Jaidev Shastri, *Virginia Tech*
Jan Jancar, *Masaryk University*
Jared Chandler, *Dartmouth College*
Jayakrishna Vadayath, *Arizona State University*
Jean-Charles Noirot Ferrand, *University of Wisconsin-Madison*
Jeroen Robben, *DistriNet, KU Leuven*
Jessy Ayala, *University of California, Irvine*
Jialuo Du, *Tsinghua University*
Jian Cui, *Indiana University Bloomington/ University of Illinois Urbana-Champaign*
Jie Ma, *Beihang University*
Jiongchi Yu, *Singapore Management University*
Joschua Schilling, *CISPA Helmholtz Center for Information Security*
Kevin Bogner, *COSIC, KU Leuven*
Keyan Guo, *University at Buffalo*
Kunsheng Tang, *University of Science and Technology of China*
Kunsong Zhao, *The Hong Kong Polytechnic University*
Kunyang Li, *University of Wisconsin-Madison*
Leming Shen, *The Hong Kong Polytechnic University*
Leonhard Balduf, *TU Darmstadt*
Marco Casagrande, *KTH Royal Institute of Technology*
Matteo Marini, *Sapienza University of Rome*
Maximilian Radoy, *Paderborn University*
Mengdie Huang, *Purdue University*
Michael Brown, *Trail of Bits*
Michele Guerra, *New York University Abu Dhabi*
Mingda Han, *Shandong University*
Mingming Zha, *Indiana University Bloomington*
Mingyi Liu, *Georgia Institute of Technology*
Mohammad Ishtiaq Ashiq Khan, *Virginia Tech*
Moritz Bley, *CISPA Helmholtz Center for Information Security*
Muhammad Ibrahim, *Georgia Institute of Technology*
Nanda Rani, *Indian Institute of Technology Kanpur*
Nico Heitmann, *Paderborn University*
Nico Schiller, *CISPA Helmholtz Center for Information Security*
Nicola Bottura, *Sapienza University of Rome*
Nicola Ruaro, *University of California, Santa Barbara*
Paul Staat, *MPI-SP*

Petar Paradžik, *University of Zagreb*
Pierre Ayoub, *LAAS-CNRS*
Prianka Mandal, *William & Mary*
Puzhuo Liu, *Ant Group & Tsinghua University*
Qiming Guo, *Texas A&M University Corpus Christi*
Rahul Kande, *Texas A&M University*
Rishit Saiya, *Cyber Defense, PwC, USA*
Robert Esswein, *University of Pittsburgh*
Ruisi Zhang, *University of California San Diego*
Runze Zhang, *Georgia Institute of Technology*
Ryan Vrecenar, *Sandia National Laboratories*
Sanket Goutam, *Stony Brook University*
Shaoyuan Xie, *University of California, Irvine*
Shashank Sharma, *Purdue University*
Shenao Yan, *University of Connecticut*
Shenghan Zheng, *Dartmouth College*
Sofiane Azogagh, *University of Quebec at Montreal*
Steven Ngo, *University of California, Irvine*
Thomas Beckx, *DistriNet, KU Leuven*
Tillson Galloway, *Georgia Tech*
Tolga Atalay, *A2 Labs LLC, Virginia Tech*
Tommaso Sacchetti, *EURECOM*
Vamsi Simhadri, *George Mason University*
Victor Olaiya, *William & Mary*
Vijayanta Jain, *University of Maine*
Vik Vanderlinden, *DistriNet, KU Leuven*
Vinny Adjibi, *Georgia Tech*
Wenhao Li, *Shandong University*
Xiang Chen, *The Hong Kong University of Science and Technology*
Xiangmin Shen, *Northwestern University*
Xin Zhang, *Peking University*
Xu He, *George Mason University*
Xuanbo Huang, *University of Science and Technology of China*
Xuesong Bai, *University of California, Irvine*
Yiming Zhang, *Tsinghua University*
Yirui He, *University of California, Irvine*
Yongkang Zhang, *Hong Kong University of Science and Technology*
Yongliang Chen, *City University of Hong Kong*
Youyeon Joo, *Seoul National University*
Yu Nong, *University at Buffalo*
Yu-Jye Tung, *The Pennsylvania State University*
Yuanhaur Chang, *Washington University in St. Louis*
Yujin Huang, *The University of Melbourne*

Zewei Shi, *The University of Melbourne; CSIRO's Data61*
Zhaoqi Xiao, *University of California, Riverside*
Zhengjie Ji, *Virginia Tech*
Zhengyao Lin, *Carnegie Mellon University*
Zhengyu Liu, *Johns Hopkins University*
Zizhuang Deng, *School of Cyber Science and Technology, Shandong University*

Ethical Review Board (ERB) Members

Thorsten Holz (Chair), *Max Planck Institute for Security and Privacy*
Adam Bates, *University of Illinois at Urbana-Champaign*
Angelos Stavrou, *Virginia Tech*
Christine Utz, *Radboud University*
Engin Kirda, *Northeastern University*
Robert Cunningham, *University of Pittsburgh*
Sebastien Bardin, *CEA List, University Paris Saclay*
Simon Birnbach, *University of Oxford*
Srdjan Capkun, *ETH Zurich*
Vincent Lenders, *University of Luxembourg*

Organizing Committee

General Chairs

Heng Yin
University of California, Riverside

Mauro Conti
University of Padua, Italy
and Örebro University, Sweden

Program Committee Co-Chairs

Hamed Okhravi
MIT Lincoln Laboratory

Ivan Martinovic
University of Oxford

Artifact Evaluation Committee Co-Chairs

Mathy Vanhoef
KU Leuven

Daniele Antonioli
EURECOM

Workshop Co-Chairs

Sébastien Bardin
CEA LIst

Christophe Hauser
Dartmouth College

Poster Session Co-Chairs

Kaushal Kafle
University of South Florida

Muslum Ozgur Ozmen
Arizona State University

Publicity Chair

Yue Xiao
IBM Research

Publications Co-Chairs

Mridula Singh
CISPA

Hyungsub Kim
Indiana University Bloomington

Sponsorship Coordinators

Yongdae Kim
KAIST

Heng Yin
University of California, Riverside

Mauro Conti
University of Padua, Italy
and Örebro University, Sweden

The Internet Society/Foundation Staff

Raquel Kroich
Event Manager

Sally Harvey
Sponsorships

Robin Wilton
Program Liaison

Robbie Mitchell
Publicity

Ivana Trbovic
Website Manager

Student Support Committee

Dan Lin (Chair)
Vanderbilt University

M. Sudha Bhuvaneswari
Damodaran College of Science

Theodore Dama
Independent reviewer

Joe Hall
Internet Society

Yu Huang
Vanderbilt University

Raquel Kroich
Internet Society Foundation

Meng Li
Hefei University of Technology

Xuan Liu
Yangzhou University

Zhuotao Liu
Tsinghua University

Meiyi Ma
Vanderbilt University

Julie Majale
Internet Society Foundation

Alejandra Prieto
Internet Society Foundation

Alan Ramirez Garcia
Independent reviewer

Claire van Zwieten
Internet Society Foundation

Robin Wilton
Internet Society

Xiaoyu Xia
RMIT University

Runhua Xu
Beihang University

Attila Yavuz
University of South Florida

Steering Group

Co-Chairs

Yongdae Kim
KAIST

Robin Wilton
Internet Society

Steering Group Members

Christopher Kruegel
UC Santa Barbara

Michael Reiter
Duke University

Wenyuan Xu
Zhejiang University

Gene Tsudik
UC Irvine

Gabriela Ciocarlie
University of Texas at San Antonio

Lorenzo Cavallaro
University College London

Daphne Yao
Virginia Tech

Anita Nikolich
UIUC

Ahmad-Reza Sadeghi
TU Darmstadt