

Proceedings

2022

**Network and Distributed
System Security Symposium**



Proceedings

2022

**Network and Distributed
System Security Symposium**

April 24-28, 2022

San Diego, CA, USA

Hosted by the
Internet Society





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

Copyright © 2022 by the Internet Society.
All rights reserved.

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

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

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

ISBN Number (Digital Format) : 1-891562-74-6

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

Session 1A: Network Protocols

ROV-MI: Large-Scale, Accurate and Efficient Measurement of ROV Deployment

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

HeadStart: Efficiently Verifiable and Low-Latency Participatory Randomness Generation at Scale

Hsun Lee, Yuming Hsu, Jing-Jie Wang, Hao Cheng Yang, and Yu-Heng Chen (National Taiwan University); Yih-Chun Hu (University of Illinois at Urbana-Champaign); Hsu-Chun Hsiao (National Taiwan University)

PMTUD is not Panacea: Revisiting IP Fragmentation Attacks against TCP

Xuewei Feng and Qi Li (Tsinghua University); Kun Sun (George Mason University); Ke Xu and Baojun Liu (Tsinghua University); Xiaofeng Zheng (Institute for Network Sciences and Cyberspace, Tsinghua University); QiAnXin Technology Research Institute & Legendsec Information Technology (Beijing) Inc.); Qiushi Yang (QiAnXin Technology Research Institute and Legendsec Information Technology (Beijing) Inc.); Haixin Duan (Institute for Network Science and Cyberspace, Tsinghua University; Qi An Xin Group Corp.); Zhiyun Qian (UC Riverside)

Subverting Stateful Firewalls with Protocol States

Amit Klein (Bar Ilan University)

Session 1B: Smartphones

PHYjacking: Physical Input Hijacking for Zero-Permission Authorization Attacks on Android

Xianbo Wang, Shangcheng Shi, Yikang Chen, and Wing Cheong Lau (The Chinese University of Hong Kong)

GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line

Yuanda Wang, Hanqing Guo, and Qiben Yan (Michigan State University)

The Droid is in the Details: Environment-aware Evasion of Android Sandboxes

Brian Kondracki, Babak Amin Azad, Najmeh Miramirkhani, and Nick Nikiforakis (Stony Brook University)

Uncovering Cross-Context Inconsistent Access Control Enforcement in Android
Hao Zhou (The Hong Kong Polytechnic University); Haoyu Wang (Beijing University of Posts and Telecommunications); Xiapu Luo (The Hong Kong Polytechnic University); Ting Chen (University of Electronic Science and Technology of China); Yajin Zhou (Zhejiang University); Ting Wang (Pennsylvania State University)

Session 1C: Cyber-crime and Forensics

Evaluating Susceptibility of VPN Implementations to DoS Attacks Using Adversarial Testing

Fabio Streun, Joel Wanner, and Adrian Perrig (ETH Zurich)

The Truth Shall Set Thee Free: Enabling Practical Forensic Capabilities in Smart Environments

Leonardo Babun, Amit Kumar Sikder, Abbas Acar, and Selcuk Uluagac (Florida International University)

LogicMEM: Automatic Profile Generation for Binary-Only Memory Forensics via Logic Inference

Zhenxiao Qi, Yu Qu, and Heng Yin (UC Riverside)

Forensic Analysis of Configuration-based Attacks

Muhammad Adil Inam and Wajih Ul Hassan (University of Illinois at Urbana-Champaign); Ali Ahad (University of Virginia); Adam Bates (University of Illinois at Urbana-Champaign); Rashid Tahir (University of Prince Mugrin); Tianyin Xu (University of Illinois at Urbana-Champaign); Fareed Zaffar (LUMS)

Session 2A: IoT and Networks

ditto: WAN Traffic Obfuscation at Line Rate

Roland Meier (ETH Zürich); Vincent Lenders (armasuisse); Laurent Vanbever (ETH Zürich)

A Lightweight IoT Cryptojacking Detection Mechanism in Heterogeneous Smart Home Networks

Ege Tekiner, Abbas Acar, and Selcuk Uluagac (Florida International University)

FANDEMIC: Firmware Attack Construction and Deployment on Power Management Integrated Circuit and Impacts on IoT Applications

Ryan Tsang, Doreen Joseph, Asmita, and Soheil Salehi (University of California, Davis); Nadir Carreon (University of Arizona); Prasant Mohapatra and Houman Homayoun (University of California, Davis)

EqualNet: A Secure and Practical Defense for Long-term Network Topology Obfuscation

Jinwoo Kim (KAIST); Eduard Marin (Telefonica Research (Spain)); Mauro Conti (University of Padua); Seungwon Shin (KAIST)

Session 2B: Fuzzing

Context-Sensitive and Directional Concurrency Fuzzing for Data-Race Detection
Zu-Ming Jiang and Jia-Ju Bai (Tsinghua University); Kangjie Lu (University of Minnesota); Shi-Min Hu (Tsinghua University)

MobFuzz: Adaptive Multi-objective Optimization in Gray-box Fuzzing
Gen Zhang, Pengfei Wang, Tai Yue, Xiangdong Kong, Shan Huang, Xu Zhou, and Kai Lu (National University of Defense Technology)

FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware
Grant Hernandez (University of Florida); Marius Muench (Vrije Universiteit Amsterdam); Dominik Maier (TU Berlin); Alyssa Milburn (Vrije Universiteit Amsterdam); Shinjo Park (TU Berlin); Tobias Scharnowski (Ruhr-University Bochum); Tyler Tucker, Patrick Traynor, and Kevin Butler (University of Florida)

EMS: History-Driven Mutation for Coverage-based Fuzzing
Chenyang Lyu and Shouling Ji (Zhejiang University); Xuhong Zhang (Zhejiang University and Zhejiang University NGICS Platform); Hong Liang (Zhejiang University); Binbin Zhao (Georgia Institute of Technology); Kangjie Lu (University of Minnesota); Raheem Beyah (Georgia Institute of Technology)

Session 2C: ML and AI #1

Tetrad: Actively Secure 4PC for Secure Training and Inference
Nishat Koti and Arpita Patra (IISc Bangalore); Rahul Rachuri (Aarhus University, Denmark); Ajith Suresh (IISc, Bangalore)

MIRROR: Model Inversion for Deep Learning Network with High Fidelity
Shengwei An, Guanhong Tao, Qiuling Xu, Yingqi Liu, and Guangyu Shen (Purdue University); Yuan Yao and Jingwei Xu (Nanjing University); Xiangyu Zhang (Purdue University)

Local and Central Differential Privacy for Robustness and Privacy in Federated Learning
Mohammad Naseri (University College London); Jamie Hayes (DeepMind); Emiliano De Cristofaro (University College London and Alan Turing Institute)

DeepSight: Mitigating Backdoor Attacks in Federated Learning Through Deep Model Inspection
Phillip Rieger, Thien Duc Nguyen, Markus Miettinen, and Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Session 3A: Web Security

Testability Tarpits: the Impact of Code Patterns on the Security Testing of Web Applications
Feras Al Kassar, Giulia Clerici, and Luca Compagna (SAP Security Research); Davide Balzarotti (EURECOM); Fabian Yamaguchi (ShiftLeft Inc)

Probe the Proto: Measuring Client-Side Prototype Pollution Vulnerabilities of One Million Real-world Websites

Zifeng Kang, Song Li, and Yinzhi Cao (Johns Hopkins University)

ScriptChecker: To Tame Third-party Script Execution With Task Capabilities

Wu Luo (Peking University); Xuhua Ding (Singapore Management University); Pengfei Wu (School of Computing, National University of Singapore); Xiaolei Zhang, Qingni Shen, and Zhonghai Wu (Peking University)

HARPO: Learning to Subvert Online Behavioral Advertising

Jiang Zhang and Konstantinos Psounis (University of Southern California); Muhammad Haroon and Zubair Shafiq (University of California, Davis)

Session 3B: Run-time Defenses

Chosen-Instruction Attack Against Commercial Code Virtualization Obfuscators

Shijia Li, Chunfu Jia, Pengda Qiu, and Qiyuan Chen (College of Computer Science, NanKai University and the Tianjin Key Laboratory of Network and Data Security Technology); Jiang Ming (University of Texas at Arlington); Debin Gao (Singapore Management University)

Building Embedded Systems Like It's 1996

Ruotong Yu (Stevens Institute of Technology, University of Utah); Francesca Del Nin (University of Padua); Yuchen Zhang and Shan Huang (Stevens Institute of Technology); Pallavi Kaliyar (Norwegian University of Science and Technology); Sarah Zacto (Cyber Independent Testing Lab); Mauro Conti (University of Padua, Delft University of Technology); Georgios Portokalidis (Stevens Institute of Technology); Jun Xu (Stevens Institute of Technology, University of Utah)

The Taming of the Stack: Isolating Stack Data from Memory Errors

Kaiming Huang and Yongzhe Huang (Penn State University); Mathias Payer (EPFL); Zhiyun Qian (UC Riverside); Jack Sampson, Gang Tan, and Trent Jaeger (Penn State University)

CFInsight: A Comprehensive Metric for CFI Policies

Tommaso Frassetto, Patrick Jauernig, David Koisser, and Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Session 3C: Cyber-physical Systems

Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks

Ziwen Wan, Junjie Shen, and Jalen Chuang (University of California, Irvine); Xin Xia (The University of California, Los Angeles); Joshua Garcia (University of California, Irvine); Jiaqi Ma (The University of California, Los Angeles); Qi Alfred Chen (University of California, Irvine)

RVPLAYER: Robotic Vehicle Forensics by Replay with What-if Reasoning

Hongjun Choi, Zhiyuan Cheng, and Xiangyu Zhang (Purdue University)

Hiding My Real Self! Protecting Intellectual Property in Additive Manufacturing Systems Against Optical Side-Channel Attacks

Sizhuang Liang (Georgia Institute of Technology); Saman Zonouz (Rutgers University); Raheem Beyah (Georgia Institute of Technology)

PoF: Proof-of-Following for Vehicle Platoons

Ziqi Xu, Jingcheng Li, and Yanjun Pan (University of Arizona); Loukas Lazos and Ming Li (University of Arizona, Tucson); Nirnimesh Ghose (University of Nebraska–Lincoln)

Session 4A: Wireless

Packet-Level Open-World App Fingerprinting on Wireless Traffic

Jianfeng Li, Shuohan Wu, Hao Zhou, and Xiapu Luo (The Hong Kong Polytechnic University); Ting Wang (Penn State); Yangyang Liu (The Hong Kong Polytechnic University); Xiaobo Ma (Xi'an Jiaotong University)

SpiralSpy: Exploring a Stealthy and Practical Covert Channel to Attack Air-gapped Computing Devices via mmWave Sensing

Zhengxiong Li (University at Buffalo, SUNY); Baicheng Chen and Xingyu Chen (University at Buffalo); Huining Li (SUNY University at Buffalo); Chenhan Xu (University at Buffalo, SUNY); Feng Lin (Zhejiang University); Chris Xiaoxuan Lu (University of Edinburgh); Kui Ren (Zhejiang University); Wenyao Xu (SUNY Buffalo)

SemperFi: Anti-spoofing GPS Receiver for UAVs

Harshad Sathaye, Gerald LaMountain, Pau Closas, and Aanjhan Ranganathan (Northeastern University)

V-Range: Enabling Secure Ranging in 5G Wireless Networks

Mridula Singh (CISPA - Helmholtz Center for Information Security); Marc Roeschlin (ETH Zurich); Aanjhan Ranganathan (Northeastern University); Srdjan Capkun (ETH Zurich)

Session 4B: Secure Computing

Hybrid Trust Multi-party Computation with Trusted Execution Environment

Pengfei Wu (School of Computing, National University of Singapore); Jianting Ning (College of Computer and Cyber Security, Fujian Normal University; Institute of Information Engineering, Chinese Academy of Sciences); Jiamin Shen, Hongbing Wang, and Ee-Chien Chang (School of Computing, National University of Singapore)

SynthCT: Towards Portable Constant-Time Code

Sushant Dinesh, Grant Garrett-Grossman, and Christopher W. Fletcher (University of Illinois at Urbana Champaign)

Binary Search in Secure Computation

Marina Blanton and Chen Yuan (University at Buffalo (SUNY))

Chunked-Cache: On-Demand and Scalable Cache Isolation for Security Architectures
Ghada Dessouky, Emmanuel Stapf, Pouya Mahmoody, Alexander Gruler, and Ahmad-Reza Sadeghi (Technical University of Darmstadt)

Session 4C: ML and AI #2

What You See is Not What the Network Infers: Detecting Adversarial Examples Based on Semantic Contradiction

Yijun Yang, Ruiyuan Gao, and Yu Li (The Chinese University of Hong Kong); Qiuxia Lai (Communication University of China); Qiang Xu (The Chinese University of Hong Kong)

Euler: Detecting Network Lateral Movement via Scalable Temporal Graph Link Prediction

Isaiah J. King and H. Howie Huang (The George Washington University)

Fooling the Eyes of Autonomous Vehicles: Robust Physical Adversarial Examples Against Traffic Sign Recognition Systems

Wei Jia and Zhaojun Lu (School of Cyber Science and Engineering, Huazhong University of Science and Technology); Haichun Zhang and Zhenglin Liu (Huazhong University of Science and Technology); Jie Wang (Shenzhen Kaiyuan Internet Security Co., Ltd); Gang Qu (University of Maryland)

FedCRI: Federated Mobile Cyber-Risk Intelligence

Hossein Fereidooni (Technical University of Darmstadt); Alexandra Dmitrienko (University of Wuerzburg); Phillip Rieger, Markus Miettinen, and Ahmad-Reza Sadeghi (Technical University of Darmstadt); Felix Madlener (KOBIL)

Session 5A: Special Problems and Use Cases

FakeGuard: Exploring Haptic Response to Mitigate the Vulnerability in Commercial Fingerprint Anti-Spoofing

Aditya Singh Rathore (University at Buffalo, SUNY); Yijie Shen (Zhejiang University); Chenhan Xu and Jacob Snyderman (University at Buffalo, SUNY); Jinsong Han and Fan Zhang (Zhejiang University); Zhengxiong Li (University of Colorado Denver); Feng Lin (Zhejiang University); Wen Yao Xu (University at Buffalo, SUNY); Kui Ren (Zhejiang University)

On Utility and Privacy in Synthetic Genomic Data

Bristena Oprisanu (UCL); Georgi Ganev (UCL and Hazy); Emiliano De Cristofaro (UCL)

ProvTalk: Towards Interpretable Multi-level Provenance Analysis in Networking Functions Virtualization (NFV)

Azadeh Tabiban and Heyang Zhao (CIISE, Concordia University, Montreal, QC, Canada); Yosr Jarraya and Makan Pourzandi (Ericsson Security Research, Ericsson Canada, Montreal, QC, Canada); Mengyuan Zhang (Department of Computing, The Hong Kong Polytechnic University, China); Lingyu Wang (CIISE, Concordia University, Montreal, QC, Canada)

Privacy in Urban Sensing with Instrumented Fleets, Using Air Pollution Monitoring As A Usecase

Ismi Abidi (IIT Delhi); Ishan Nangia (MPI-SWS); Paarijaat Aditya (Nokia Bell Labs); Rijurekha Sen (IIT Delhi)

Session 5B: Cloud and Edge Computing

Titanium: A Metadata-Hiding File-Sharing System with Malicious Security

Weikeng Chen (DZK/UC Berkeley); Thang Hoang (Virginia Tech); Jorge Guajardo (Robert Bosch Research and Technology Center); Attila A. Yavuz (University of South Florida)

Remote Memory-Deduplication Attacks

Martin Schwarzl, Erik Kraft, Moritz Lipp, and Daniel Gruss (Graz University of Technology)

Interpretable Federated Transformer Log Learning for Cloud Threat Forensics

Gonzalo De La Torre Parra (University of the Incarnate Word, TX, USA); Luis Selvera (Secure AI and Autonomy Lab, The University of Texas at San Antonio, TX, USA); Joseph Khoury (The Cyber Center For Security and Analytics, University of Texas at San Antonio, TX, USA); Hector Irizarry (Raytheon, USA); Elias Bou-Harb (The Cyber Center For Security and Analytics, University of Texas at San Antonio, TX, USA); Paul Rad (Secure AI and Autonomy Lab, The University of Texas at San Antonio, TX, USA)

Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks

Chongzhou Fang, Han Wang, and Najmeh Nazari (University of California, Davis); Behnam Omid (George Mason University); Avesta Sasan (University of California, Davis); Khaled N. Khasawneh (George Mason University); Setareh Rafatirad and Houman Homayoun (University of California, Davis)

Session 5C: Attacks on ML/AI

ATTEQ-NN: Attention-based QoE-aware Evasive Backdoor Attacks

Xueluan Gong (Wuhan University); Yanjiao Chen (Zhejiang University); Jianshuo Dong and Qian Wang (Wuhan University)

RamBoAttack: A Robust and Query Efficient Deep Neural Network Decision Exploit

Viet Quoc Vo and Ehsan Abbasnejad (The University of Adelaide); Damith C. Ranasinghe (University of Adelaide)

Property Inference Attacks Against GANs

Junhao Zhou, Yufei Chen, and Chao Shen (Xi'an Jiaotong University); Yang Zhang (CISPA Helmholtz Center for Information Security)

Get a Model! Model Hijacking Attack Against Machine Learning Models

Ahmed Salem, Michael Backes, and Yang Zhang (CISPA Helmholtz Center for Information Security)

Session 6A: Privacy and Anonymity

DRAWN APART: A Device Identification Technique based on Remote GPU Fingerprinting

Tomer Laor (Ben-Gurion Univ. of the Negev); Naif Mehanna and Antonin Durey (Univ. Lille, CNRS, Inria); Vitaly Dyadyuk (Ben-Gurion Univ. of the Negev); Pierre Laperdrix and Clémentine Maurice (Univ. Lille, CNRS, Inria); Yossi Oren (Ben-Gurion Univ. of the Negev); Romain Rouvoy (Univ. Lille, CNRS, Inria / IUF); Walter Rudametkin (Univ. Lille, CNRS, Inria); Yuval Yarom (University of Adelaide)

Clarion: Anonymous Communication from Multiparty Shuffling Protocols

Saba Eskandarian (University of North Carolina at Chapel Hill); Dan Boneh (Stanford University)

VPNalyzer: Systematic Investigation of the VPN Ecosystem

Reethika Ramesh (University of Michigan); Leonid Evdokimov (Independent); Diwen Xue and Roya Ensafi (University of Michigan)

hbACSS: How to Robustly Share Many Secrets

Thomas Yurek and Licheng Luo (University of Illinois at Urbana-Champaign); Jaiden Fairoze (University of California, Berkeley); Aniket Kate (Purdue University); Andrew Miller (University of Illinois at Urbana-Champaign)

Session 6B: Kernel Security

An In-depth Analysis of Duplicated Linux Kernel Bug Reports

Dongliang Mu (Huazhong University of Science and Technology); Yuhang Wu, Yueqi Chen, and Zhenpeng Lin (Pennsylvania State University); Chensheng Yu (George Washington University); Xinyu Xing (Pennsylvania State University); Gang Wang (University of Illinois at Urbana-Champaign)

Kasper: Scanning for Generalized Transient Execution Gadgets in the Linux Kernel

Brian Johannismeyer and Jakob Koschel (VU Amsterdam); Kaveh Razavi (ETH Zurich); Herbert Bos and Cristiano Giuffrida (VU Amsterdam)

Semantic-Informed Driver Fuzzing Without Both the Hardware Devices and the Emulators

Wenjia Zhao (Xi'an Jiaotong University and University of Minnesota); Kangjie Lu and Qiushi Wu (University of Minnesota); Yong Qi (Xi'an Jiaotong University)

Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel

Yizhuo Zhai, Yu Hao, Zheng Zhang, Weiteng Chen, Guoren Li, Zhiyun Qian, Chengyu Song, Manu Sridharan, and Srikanth V. Krishnamurthy (University of California, Riverside); Trent Jaeger (The Pennsylvania State University); Paul Yu (U.S. Army Research Laboratory)

Session 6C: Keys and Authentication

F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure

Laurent Chuat (ETH Zurich); Cyrill Krähenbühl (ETH Zurich); Prateek Mittal (Princeton University); Adrian Perrig (ETH Zurich)

Let's Authenticate: Automated Certificates for User Authentication

James Connors, Corey Devenport, Stephen Derbidge, Natalie Farnsworth, Kyler Gates, Stephen Lambert, Christopher McClain, Parker Nichols, and Daniel Zappala (Brigham Young University)

Transparency Dictionaries with Succinct Proofs of Correct Operation

Ioanna Tzialla (New York University); Abhiram Kothapalli and Bryan Parno (Carnegie Mellon University); Srinath Setty (Microsoft Research)

Session 7A: Blockchains

Multi-Certificate Attacks against Proof-of-Elapsed-Time and Their Countermeasures

Huibo Wang (Baidu Security); Guoxing Chen (Shanghai Jiao Tong University); Yinqian Zhang (Southern University of Science and Technology); Zhiqiang Lin (Ohio State University)

Shaduf: Non-Cycle Payment Channel Rebalancing

Zhonghui Ge, Yi Zhang, Yu Long, and Dawu Gu (Shanghai Jiao Tong University)

NC-Max: Breaking the Security-Performance Tradeoff in Nakamoto Consensus

Ren Zhang, Dingwei Zhang, and Quake Wang (Nervos); Shichen Wu (School of Cyber Science and Technology, Shandong University); Jan Xie (Nervos); Bart Preneel (imec-COSIC, KU Leuven)

Speeding Dumbo: Pushing Asynchronous BFT Closer to Practice

Bingyong Guo (Institute of Software, Chinese Academy of Sciences); Yuan Lu (Institute of Software Chinese Academy of Sciences); Zhenliang Lu and Qiang Tang (The University of Sydney); Jing Xu and Zhenfeng Zhang (Institute of Software, Chinese Academy of Sciences)

Session 7B: Software Components and Interactions

Preventing Kernel Hacks with HAKCs

Derrick McKee (Purdue University); Yianni Giannaris, Carolina Ortega, and Howard Shrobe (MIT CSAIL); Mathias Payer (EPFL); Hamed Okhravi and Nathan Burow (MIT Lincoln Laboratory)

D-Box: DMA-enabled Compartmentalization for Embedded Applications

Alejandro Mera, Yi Hui Chen, Ruimin Sun, Engin Kirda, and Long Lu (Northeastern University)

Cross-Language Attacks

Samuel Mergendahl, Nathan Burow, and Hamed Okhravi (MIT Lincoln Laboratory)

COOPER: Testing the Binding Code of Scripting Languages with Cooperative Mutation

Peng Xu (TCA/SKLCS, Institute of Software, Chinese Academy of Sciences; University of Chinese Academy of Sciences); Yanhao Wang (QI-ANXIN Technology Research Institute); Hong Hu (Pennsylvania State University); Purui Su (TCA/SKLCS, Institute of Software, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences)

Session 7C: Human Factors

Demystifying Local Business Search Poisoning for Illicit Drug Promotion

Peng Wang, Zilong Lin, Xiaojing Liao, and XiaoFeng Wang (Indiana University Bloomington)

Hazard Integrated: Understanding Security Risks in App Extensions to Team Chat Systems

Mingming Zha (Indiana University Bloomington); Jice Wang (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences); Yuhong Nan (Sun Yat-sen University); Xiaofeng Wang (Indiana University Bloomington); Yuqing Zhang and Zelin Yang (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences)

Above and Beyond: Organizational Efforts to Complement U.S. Digital Security Compliance Mandates

Rock Stevens (University of Maryland); Faris Bugra Kokulu and Adam Doupe (Arizona State University); Michelle L. Mazurek (University of Maryland)

Fighting Fake News in Encrypted Messaging with the Fuzzy Anonymous Complaint Tally System (FACTS)

Linsheng Liu (George Washington University); Daniel S. Roche (United States Naval Academy); Austin Theriault and Arkady Yerukhimovich (George Washington University)

Message from the General Chair

Welcome to the 2022 Network and Distributed System Security (NDSS) Symposium!

This year marks our first year trying a hybrid event. We are excited to have an in-person symposium again, while still including those who are unable to travel, and we hope to provide an exceptional experience to both sets of participants! This year, we have an amazing program featuring a stellar line-up of research papers, six workshops, two poster sessions (one in person and one virtual), and two exciting keynote speakers.

NDSS 2022 has continued the tradition of having two submission phases. The Program Committee Co-Chairs Farinaz Koushanfar and Wenyuan Xu have done a wonderful job putting together the program, and I'd like to thank them for their tireless efforts. I would also like to thank the program committee members and the external reviewers for their work in creating an exciting program, and our publications chair, David Balenson, for pulling the papers together to be published.

Thanks also to Yasemin Acar and Ben Stock for bringing together a great set of associated workshops and symposium. This year, we have five workshops - three on Sunday, April 24, and two on Thursday, April 28 – and our first ever symposium on Thursday. The associated events this year are:

- 1) Automotive and Autonomous Vehicle Security (AutoSec) Workshop;
- 2) Fuzzing Workshop;
- 3) Binary Analysis Research (BAR) Workshop;
- 4) Learning from Authoritative Security Experiment Results (LASER) Workshop;
- 5) Measurements, Attacks, and Defenses for the Web (MADWeb) Workshop;
- and
- 6) Usable Security and Privacy (USEC) Symposium.

Four of the workshops continue from last year, one is entirely new, and we're thrilled to welcome USEC back to NDSS as a symposium rather than a workshop.

I'm also excited that we have a poster session again this year and would like to thank Xiaojing Liao and Alexandra Dmitrienko for putting it together. Thank you especially for the effort to have not one, but two, poster sessions, so that both our in-person and virtual attendees and poster presenters can participate.

There are many other people who have contributed to making NDSS 2022 a success. I would like to thank Stefanie Roos and her team for reviewing the student grant applications, Brendan Saltaformaggio and Ramjita Pai Kasturi for publicity, Lujo Bauer and his team for reviewing papers for the Test of Time award, Robert Broberg as sponsorship chair, and Tom Hutton as local arrangements chair. I would also like to thank the Steering Group for providing sage recommendations and feedback throughout the year.

NDSS is possible in large part thanks to our generous sponsors. I'd like to thank (in alphabetical order) sponsorship from the following companies: Baidu, ByteDance, Check Point, Futurewei Technologies, Google, Homelight, IBM, Intel Security, Microsoft Research, National Science Foundation, Netflix, Novi, Palo Alto Networks, Qualcomm, Resecurity, Team Cymru, and Technology Innovation Institute (TII).

An especially huge thank you to Karen O'Donoghue and her team for all the work performed behind the scenes, especially during the challenges of Covid and our first ever hybrid event! Thank you to the Internet Society for their ongoing support of NDSS, and to the Association Management Solutions (AMS) staff.

And lastly, thank you to everyone who is participating in the symposium for your patience as we changed dates due to Covid, and work to make a hybrid event a success. I hope that you all enjoy NDSS 2022!

Carrie Gates
General Chair, NDSS 2022

Message from the Program Committee Co-Chairs

It is our great pleasure to present to you the technical program of the Annual Network and Distributed System Security (NDSS) Symposium 2022, held as a hybrid event on April 24-28, 2022. For the past 29 years NDSS has established itself as one of the top conferences in systems and network security. Papers published at NDSS have made significant impact on research and practice, as exemplified by the awardees of the NDSS Test-of-Time Award. Our goal continues to be “impact”, especially in the form of novel and practical solutions and techniques in cyber security. We hope that the papers in this year’s program reflect the same strong potential in securing real-world networks and systems.

This year we received a total of 513 complete submissions (i.e., not counting papers that clearly violated the submission guidelines). Submissions were evaluated on the basis of their technical quality, novelty, and significance. Multiple rounds of reviewing culminated in a one-day online program committee meeting on October 21, 2021. At the end of the review process, 83 papers (16.2% acceptance rate) were selected to appear in the program. We strove to make the review process a competitive but constructive one. Program Committee (PC) members were regularly reminded to identify positive points in a submission and provide concrete suggestions to improve each paper. As we did last year, we took the approach of having three reviews per paper in the first review round to guarantee higher assurance of early decisions. Later for each author rebuttal, which was solicited after all reviews were in, we required the corresponding reviews be updated to respond to the rebuttal, to help improve the quality, timeliness, and responsiveness of the review process.

Organizing a conference as large as NDSS is a substantial endeavor, and we would like to extend our sincere thanks to everyone who contributed her or his time and effort. We would like to specifically thank a few individuals who made particular contributions to NDSS 2022. General Chair Carrie Gates oversaw the conference and worked closely with us for Keynote Speaker. Karen O'Donoghue served as a critical interface between the Program Co-Chairs, the Organizing Committee and ISOC. Publicity Chair Brendan Saltaformaggio worked seamlessly with us to solicit submissions and promote the conference. Publications Chair David Balenson took excellent care of the proceedings production matters. Due to the pandemic the PC meeting was conducted online, this year we switched to a one-day single-track schedule with success. Our special thanks also go to Chen Yan from Zhejiang University for continuous effort in maintaining the submission system, supporting the PC Co-Chairs during the reviewing process, and planning the event schedule.

Last but not least, we would like to thank our PC members and the external reviewers. The PC members have contributed significant time and effort to the creation of the technical program. It has been our privilege working with them. Finally, we thank all authors who submitted to NDSS 2022 and all attendees who are virtually joining us at NDSS 2022, without whom NDSS would not be possible. Enjoy the conference!

Farinaz Koushanfar and Wenyuan Xu
Program Co-Chairs, NDSS 2022

Message from the Internet Society

The Internet Society is proud, once again, to host the Network and Distributed System Security (NDSS) Symposium, one of the world's premier academic research conferences on network and distributed system security. Our involvement with the NDSS Symposium spans 29 years, a true testament to the importance, global support, and longevity of this annual event.

A key focus of the Internet Society is improving the security and trustworthiness of the global open Internet. In order to promote this trust, we need new ideas and quality research on the security and privacy of our connected devices, as well as the Internet that brings them together. NDSS 2022 will highlight the latest innovations and research on security and privacy and will give researchers a platform to collaborate further on their work. The symposium, with its focus on student participation, will also help to foster the next generation of leaders in the fields of security and privacy.

After two years of a global pandemic, NDSS 2022 will be the first ever hybrid NDSS symposium. We are excited that some of you will be able to meet face-to-face again in 2022 while those who are virtual will have full access to the program. The program committee and event organization team have put together an exceptional agenda for the online symposium. This agenda is a full five days including five co-located workshops (AutoSec, BAR, FUZZING, MADWeb, and LASER), a co-located symposium (USEC), 83 paper presentations, two exciting keynotes, and 34 posters. The two keynotes this year are particularly important and timely topics. Alex Gantman will open the symposium discussing Measuring Security Outcomes. On Wednesday, Srin Devadas will explore the question: "Will Cryptographically-secure Anonymous Communication Ever be Practical?"

NDSS 2022 is a valuable gathering of security researchers and professionals from around the globe. We are extremely grateful for the hard work and countless hours that the General Chair Carrie Gates, Program Committee Co-chairs Farinaz Koushanfar and Wenyan Xu, and other members of the Organizing Committee have invested putting together the event. We also thank the reviewers and volunteers who helped prepare the many aspects of the event. Finally, we thank all our sponsors without whom this conference would not be possible. This includes our Platinum sponsor the National Science Foundation; our Gold sponsors Baidu, Google, and Technology Innovation Institute; our T-shirt sponsor IBM; our Silver sponsors ByteDance, Checkpoint, FutureWei Technologies, Intel Security, Microsoft Research, Netflix, Novi, Palo Alto Networks, Qualcomm, Resecurity, and Team Cymru; and our Supporting sponsor Homelight.

On behalf of the Internet Society, I welcome you to NDSS 2022. I hope you have an enjoyable and productive week.

Andrew Sullivan
CEO, Internet Society

Program Committee

Farinaz Koushanfar, *University of California, San Diego* (Program Co-Chair)

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

Adam Doupe, *Arizona State University*

Adwait Nadkarni, *William & Mary*

Ahmad-Reza Sadeghi, *Technical University of Darmstadt*

Alexandra Dmitrienko, *University of Wuerzburg*

Alvaro Cardenas, *UC Santa Cruz*

Antonio Bianchi, *Purdue University*

Arthur Gervais, *Imperial College London*

Avesta Sasan, *University of California Davis*

Aysajan Abidin, *imec-COSIC, KU Leuven*

Ben Stock, *CISPA Helmholtz Center for Information Security*

Benjamin Andow, *Google*

Berkay Celik, *Purdue University*

Bitar Rouhani, *Microsoft*

Brendan Saltaformaggio, *Georgia Institute of Technology*

Brent ByungHoon Kang, *KAIST*

Chao Shen, *Xi'an Jiaotong University*

Christopher Liebchen, *Google*

Cornelius Aschermann, *Ruhr-Universität Bochum*

Dan Wallach, *Rice*

Daniel Holcomb, *University of Massachusetts Amherst*

Dongyan Xu, *Purdue University*

Emiliano De Cristofaro, *University College London*

Gang Qu, *University of Maryland*

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

Guofei Gu, *Texas A&M*

Haixin Duan, *Tsinghua University*

Hamed Okhravi, *MIT Lincoln Laboratory*

Haojin Zhu, *Shanghai Jiao Tong University*

Hong Hu, *Pennsylvania State University*

Houman Homayoun, *UC Davis*

Ivan De Oliveira Nunes, *Rochester Institute of Technology*

Jeyavijayan Rajendran, *Texas A&M University*

Joel Frank, *Ruhr-Universität Bochum*

Johanna Sepulveda, *Airbus Defence and Space*

Kangjie Lu, *University of Minnesota*

Kapil Singh, *IBM T.J. Watson Research Center*

Katharina Kohls, *Radboud University*

Kun Sun, *George Mason University*

Lannan Luo, *University of South Carolina*
Lejla Batina, *Radboud University*
Limin Jia, *CMU*
Lucas Davi, *University of Duisburg-Essen*
Maliheh Shirvanian, *Visa Research*
Manuel Egele, *Boston University*
Marcus Peinado, *Microsoft Research*
Markus Miettinen, *Technical University of Darmstadt*
Mathias Payer, *EPFL*
Mauro Conti, *University of Padua*
Michael Franz, *University of California, Irvine*
Minhui, Jason Xue, *The University of Adelaide*
Neil Gong, *Duke University*
Nele Mentens, *Leiden University and KU Leuven*
Ning Zhang, *Washington University in St. Louis*
Norrathep Rattanavipanon, *Prince of Songkla University, Phuket Campus*
Pedro Moreno-Sanchez, *IMDEA Software Institute*
Qi Alfred Chen, *UC Irvine*
Qi Li, *Tsinghua University*
Qian Wang, *Wuhan University*
Qiang Zeng, *University of South Carolina*
Ren Zhang, *Nervos*
Ryan Gerdes, *Virginia Tech*
Saman Zonouz, *Rutgers University*
Samuel Jero, *MIT Lincoln Laboratory*
Samuel Marchal, *Aalto University and F-Secure Corporation*
Sazzadur Rahaman, *University of Arizona*
Selcuk Uluagac, *Florida International University*
Shouling Ji, *Zhejiang University*
Sooel Son, *KAIST*
Srdjan Capkun, *ETH Zurich*
Srinath Setty, *Microsoft Research*
Stefanie Roos, *TU Delft*
Stjepan Picek, *TU Delft*
Syed Rafiul Hussain, *Pennsylvania State University*
Tiffany Bao, *Arizona State University*
Ting Chen, *University of Electronic Science and Technology of China*
Trent Jaeger, *Penn State University*
Xiaojing Liao, *Indiana University Bloomington*
Xiaoyu Ji, *Zhejiang University*
Xiapu Luo, *The Hong Kong Polytechnic University*
Xinyang Ge, *Microsoft Research*
Yanjiao Chen, *Zhejiang University*

Yier Jin, *University of Florida*
Yiorgos Makris, *UT Dallas*
Yongdae Kim, *KAIST*
Yuan Tian, *University of Virginia*
Zahra Ghodsi, *UC San Diego*
Zhenkai Liang, *National University of Singapore*
Zhou Li, *University of California, Irvine*

External Reviewers

Abbas Acar, *Florida International University*
Aditya Basu, *Pennsylvania State University*
Adrian Dabrowski, *UC Irvine*
Ahmet Aris, *Florida International University*
Alessandro Brighente, *University of Padua*
Amit Seal Ami, *William & Mary*
Anis Yusof, *National University of Singapore*
Arish Sateesan, *KU Leuven*
Baojun Liu, *Tsinghua University*
Changhun Song, *KAIST*
Chaoyi Lu, *Tsinghua University*
Christian Niesler, *University of Duisburg-Essen*
Christopher Orsini, *North Carolina State University*
Chuji Zhang, *National University of Singapore*
Darion Cassel, *Carnegie Mellon University*
David Gens, *UC Irvine*
David Paaßen, *University of Duisburg-Essen*
David Reinoso, *Pennsylvania State University*
Deliang Chang, *Tsinghua University*
Dimitrios Vasilopoulos, *IMDEA Software Institute*
Dipanjan Das, *UC Santa Barbara*
Dohyun Kim, *KAIST*
Dongkwan Kim, *KAIST*
Erik Pohle, *imec-COSIC KU Leuven*
Eunsoo Kim, *KAIST*
Frank Capobianco, *Pennsylvania State University*
Gaurav Somani, *Central University of Rajasthan*
Han Zhang, *Carnegie Mellon University*
Ignacio Cascudo, *IMDEA Software Institute*
Jaehoon Kim, *KAIST*
Jens-Rene Giesen, *University of Duisburg-Essen*
Jiacen Xu, *UC Irvine*
Jiahao Liu, *National University of Singapore*
Jianwei Huang, *Texas A&M University*
Jo Vliegen, *KU Leuven*
Joann Qiongna Chen, *UC Irvine*
Joonha Jang, *KAIST*
Jun Zeng, *National University of Singapore*
Kaihang Ji, *National University of Singapore*
Kaiming Huang, *Pennsylvania State University*
Kaiwen Shen, *Tsinghua University*
Kaushal Kafle, *William & Mary*

Kevin Hong, *Texas A&M University*
Laurens Le Jeune, *KU Leuven*
Leila Delshadtehrani, *Boston University*
Mangi Cho, *KAIST*
Mariusz Jakubowski, *Microsoft Research*
Matteo Cardaioli, *University of Padua*
Maverick Woo, *Carnegie Mellon University*
Md Masoom Rabbani, *KU Leuven*
Michael Rodler, *University of Duisburg-Essen*
Mincheol Son, *KAIST*
Mingming Zhang, *Tsinghua University*
Mingxuan Liu, *Tsinghua University*
Muoi Tran, *National University of Singapore*
Ning Zhang, *Washington University in St. Louis*
Phakpoom Chinprutthiwong, *Texas A&M University*
Prashast Srivastava, *Purdue University*
Qifan Zhang, *UC Irvine*
Qixiao Lin, *Beihang University*
Rahul George, *Pennsylvania State University*
Riccardo Lazzeretti, *Sapienza University of Rome*
Sangwook Bae, *KAIST*
Sashidhar Jakkamsetti, *UC Irvine*
Satwik Prabhu Kumble, *TU Delft*
Sebastian Surminski, *University of Duisburg-Essen*
Seoyeon Hwang, *UC Irvine*
Shichen Wu, *Shandong University*
Shu Wang, *George Mason University*
Sunil Manandhar, *William & Mary*
Tao Wan, *Carleton University*
Tobias Cloosters, *University of Duisburg-Essen*
Tommy Chen, *George Mason University*
Varun Madathil, *North Carolina State University*
Xiao Sui, *Shandong University*
Xiaorui Pan, *Google*
Xinda Wang, *George Mason University*
Xu He, *George Mason University*
Yangyong Zhang, *Texas A&M University*
Yanmao Man, *University of Arizona*
Yoshimichi Nakatsuka, *UC Irvine*
Yuncong Zhang, *Shanghai Jiao Tong University*
Yu-Tsung Lee, *Pennsylvania State University*
Yiming Zhang, *Tsinghua University*
Zhe Zhou, *Fudan University*
Zhijie Ren, *Shanghai Shanda Networking Development Co. Ltd.*

Organizing Committee

General Chair

Carrie Gates
Bank of America

Program Committee Co-Chairs

Farinaz Koushanfar
University of California, San Diego

Wenyuan Xu
Zhejiang University

Workshop Co-Chairs

Yasemin Acar
Leibniz University Hannover

Ben Stock
*CISPA Helmholtz Center for
Information Security*

Poster Session Co-Chairs

Alexandra Dmitrienko
University of Würzburg

Xiaoqing Liao
Indiana University

Student Support Committee

Stefanie Roos (Chair)
TU Delft

Pedro Moreno-Sanchez
IMDEA Software Institute

Arthur Gervais
Imperial College London

Jason Xue
University of Adelaide

Sazzadur Rahaman
University of Arizona

Yanjiao Chen
Zhejiang University

Test of Time Award Committee

Lujo Bauer (Chair)
Carnegie Mellon University

Trent Jaeger
Pennsylvania State University

Alina Oprea
Northeastern University

Yongdae Kim
KAIST

Michael K. Reiter
U. North Carolina at Chapel Hill

Engin Kirda
Northeastern University

Deborah Shands
SRI International

Publicity Co-Chairs

Brendan Saltaformaggio
Georgia Institute of Technology

Ranjita Pai Kastrui
Georgia Tech

Historian and Publications Chair

David Balenson
SRI International

Sponsorship Chair

Robert Broberg
Nanograss Photonics

Past General Chair

Trent Jaeger
Pennsylvania State University

Local Arrangements Chair

Thomas Hutton
San Diego Supercomputer Center

Event Manager

Karen O'Donoghue
Internet Society

Steering Group

Co-Chairs

Carrie Gates
Bank of America

Karen O'Donoghue
Internet Society

Steering Group Members

David Balenson
SRI International

Zhenkai Liang
National University of Singapore

Gabriela Ciocarlie
University of Texas San Antonio

Sarah Meiklejohn
University College London

Tom Hutton
San Diego Supercomputer Center

Alina Oprea
Northeastern University

Trent Jaeger
Pennsylvania State University

Deborah Shands
SRI International

Farinaz Koushanfar
University of California, San Diego

Dongyan Xu
Purdue University

Chris Kruegel
University of California, Santa Barbara