NDSS 2022 Accepted Papers

[Review the session schedule](https://www.ndss-symposium.org/wp-content/uploads/SessionsSchedule.pdf) and learn when papers will be presented during the Symposium.

The following papers are currently accepted for NDSS 2022:

Summer Cycle

**Property Inference Attacks Against GANs**Junhao Zhou, Yufei Chen, and Chao Shen (Xi’an Jiaotong University); Yang Zhang (CISPA Helmholtz Center for Information Security)

**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)

**Subverting Stateful Firewalls with Protocol States**Amit Klein (Bar Ilan 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 & Alan Turing Institute)

**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)

**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)

**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)

**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)

**Get a Model! Model Hijacking Attack Against Machine Learning Models**Ahmed Salem, Michael Backes, and Yang Zhang (CISPA Helmholtz Center for Information Security)

**SemperFi: Anti-spoofing GPS Receiver for UAVs**Harshad Sathaye, Gerald LaMountain, Pau Closas, and Aanjhan Ranganathan (Northeastern University)

**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)

**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)

**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)

**Binary Search in Secure Computation**Marina Blanton and Chen Yuan (University at Buffalo (SUNY))

**Above and Beyond: Organizational Efforts to Complement U.S. Digital Security Compliance Mandates**Rock Stevens (University of Maryland); Faris Bugra Kokulu and Adam Doupé (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)

**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)

**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)

**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)

**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)

**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)

**Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks**Chongzhou Fang, Han Wang, and Najmeh Nazari (University of California, Davis); Behnam Omidi (George Mason University); Avesta Sasan (University of California, Davis); Khaled N. Khasawneh (George Mason University); Setareh Rafatirad and Houman Homayoun (University of California, Davis)

**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)

**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)

**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)

**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)

**EMS: History-Driven Mutation for Coverage-based Fuzzing**Chenyang Lyu and Shouling Ji (Zhejiang University); Xuhong Zhang (Zhejiang University & 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)

**CFInsight: A Comprehensive Metric for CFI Policies**Tommaso Frassetto, Patrick Jauernig, David Koisser, and Ahmad-Reza Sadeghi (Technical University of Darmstadt)

**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)

Fall Cycle

**What You See is Not What the Network Infers: Detecting Adversarial Examples Based on Semantic Contradiction**  
Yijun YANG, RuiYuan Gao, YU LI, Qiuxia Lai, and Qiang Xu (The Chinese University of Hong Kong)

**ATTEQ-NN: Attention-based QoE-aware Evasive Backdoor Attacks**Xueluan Gong (Wuhan University); Yanjiao Chen (Zhejiang University); Jianshuo Dong and Qian Wang (Wuhan University)

**Chosen-Assembly 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)

**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)

**Building Embedded Systems Like It’s 1996**Ruotong Yu (Stevens Institute of Technology); Francesca Del Nin (University of Padua); Yuchen Zhang and Shan Huang (Stevens Institute of Technology); Pallavi Kaliyar (University of Padua); Sarah Zakto (Cyber Independent Testing Lab); Mauro Conti (University of Padua); Georgios Portokalidis and Jun Xu (Stevens Institute of Technology)

**Evaluating Susceptibility of VPN Implementations to DoS Attacks Using Adversarial Testing**Fabio Streun, Joel Wanner, and Adrian Perrig (ETH Zurich)

**D-Box: DMA-enabled compartmentalization for embedded applications**Alejandro Mera, Yi Hui Chen, Ruimin Sun, Engin Kirda, and Long Lu (Northeastern University)

**ditto: WAN Traffic Obfuscation at Line Rate**Roland Meier (ETH Zürich); Vincent Lenders (armasuisse); Laurent Vanbever (ETH Zürich)

**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)

**Cross-Language Attacks**Samuel Mergendahl, Nathan Burow, and Hamed Okhravi (MIT Lincoln Laboratory)

**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 at Buffalo, SUNY); Feng Lin (Zhejiang University); Wenyao Xu (University at Buffalo, SUNY); Kui Ren (Zhejiang University)

**On Utility and Privacy in Synthetic Genomic Data**Bristena Oprisanu (UCL); Georgi Ganev (UCL & Hazy); Emiliano De Cristofaro (UCL)

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

**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)

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

**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)

**Clarion: Anonymous Communication from Multiparty Shuffling Protocols**Saba Eskandarian (University of North Carolina at Chapel Hill); Dan Boneh (Stanford University)

**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)

**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)

**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)

**A Metadata-Hiding File-Sharing System with Malicious Security**Weikeng Chen (UC Berkeley); Thang Hoang (Virginia Tech); Jorge Guajardo (Robert Bosch Research and Technology Center); Attila A. Yavuz (University of South Florida)

**To Trust or Not to Trust: Hybrid Multi-party Computation with Trusted Execution Environment**Pengfei Wu and Ee-Chien Chang (School of Computing, National University of Singapore); Jianting Ning (Fujian Normal University); Hongbin Wang and Jiamin Shen (School of Computing, National University of Singapore)

**Systematic Discovery of Denial-of-Service 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)

**RamBoAttack: A Robust and Query Efficient Deep Neural Network Decision Exploit**viet vo (The University of Adelaide); Damith C. Ranasinghe (University of Adelaide); Ehsan Abbasnejad (The University of Adelaide)

**Shaduf: Non-Cycle Payment Channel Rebalancing**Zhonghui Ge, Yi Zhang, Yu Long, and Dawu Gu (Shanghai Jiao Tong University)

**A Lightweight IoT Cryptojacking Detection Mechanism in Heterogeneous Smart Home Networks**Ege Tekiner, Abbas Acar, and Selcuk Uluagac (Florida International University)

**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)

**ROV-MI: Large-Scale, Accurate and Efficient Measurement of ROV Deployment**Wenqi Chen (Tsinghua University); Zhiliang Wang (wzl@cernet.edu.cn); Dongqi Han (Institute for Network Sciences and Cyberspace, Tsinghua University); Chenxin Duan, Xia Yin, Jiahai Yang, and Xingang Shi (Tsinghua University)

**SynthCT: Towards Portable Constant-Time Code**Sushant Dinesh, Grant Garrett-Grossman, and Christopher W. Fletcher (University of Illinois at Urbana Champaign)

**KASPER: Scanning for Generalized Transient Execution Gadgets in the Linux**Kernel Brian Johannesmeyer, Jakob Koschel, and Cristiano Giuffrida (Vrije Universiteit Amsterdam); Kaveh Razavi (ETH Zurich); Herbert Bos (Vrije Universiteit Amsterdam)

**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)

**F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure**Laurent Chuat (ETH Zurich); Cyrill Krähenbühl (ETH Zürich); Prateek Mittal (Princeton University); Adrian Perrig (ETH Zurich)

**RVPLAYER: Robotic Vehicle Forensics by Replay with What-if Reasoning**Hongjun Choi, Zhiyuan Cheng, and Xiangyu Zhang (Purdue University)

**GhostTalk: Interactive Attack on Smartphone Voice Assistant Through Power Line Side-Channel**Yuanda Wang, Hanqing Guo, and Qiben Yan (Michigan State University)

**Let’s Authenticate: Automated Certificates for User Authentication**James Conners, Stephen Derbidge, Natalie Farnsworth, Kyler Gates, Stephen Lambert, Christopher McClain, and Daniel Zappala (Brigham Young University)

**Demystifying Local Business Search Poisoning for Illicit Drug Promotion**Peng Wang, Zilong Lin, Xiaojing Liao, and XiaoFeng Wang (Indiana University Bloomington)

**VPNInspector: Systematic Investigation of the VPN Ecosystem**Reethika Ramesh (University of Michigan); Leonid Evdokimov (Independent); Diwen Xue and Roya Ensafi (University of Michigan)

**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)

**Hiding My Real Self! Protecting 3D Printer Intellectual Property Against Optical Side-Channel Attacks**Sizhuang Liang (Georgia Institute of Technology); Saman Zonouz (Rutgers University); Raheem Beyah (Georgia Institute of Technology)

**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)

**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)

**LogicMEM: Automatic Profile Generation for Binary-Only Memory Forensics via Logic Inference**Zhenxiao Qi, Yu Qu, and Heng Yin (UC Riverside)

**MIRROR: Model Inversion for Deep LearningNetwork 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)

**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)

**FANDEMIC: Firmware Attack Construction and Deployment on Power Management IC and Impacts on IoT Applications**Ryan Tsang, Doreen Joseph, Asmita Jha, and Soheil Salehi (University of California, Davis); Nadir Carreon (University of Arizona); Prasant Mohapatra and Houman Homayoun (University of California, Davis)

**COOPER: Testing the Binding Code of Scripting Languages with Cooperative Mutation**Peng Xu (Institute of Software/CAS China; University of Chinese Academy of Sciences); Wang Yanhao (QI-ANXIN Technology Research Institute); Hong Hu (Penn State University); Purui Su (Institute of Software/CAS China)

**NC-Max: Breaking the Security-Performance Tradeoff in Nakamoto Consensus**Ren Zhang, Dingwei Zhang, and Quake Wang (Nervos); Shichen Wu (Shandong University); Jan Xie (Nervos); Bart Preneel (imec-COSIC, KU Leuven)

**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)

**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 & Legendsec Information Technology (Beijing) Inc.); Haixin Duan (Institute for Network Science and Cyberspace, Tsinghua University; Qi An Xin Group Corp.); Zhiyun Qian (UC Riverside)

**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)

**Speeding Dumbo: Pushing Asynchronous BFT 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 (Institute of Software, Chinese Academy of Sciences); Zhenfeng Zhang (TCA of State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences)

**Hazard Integrated: Understanding Security Risks in App Extensions to Team Chat Systems**Mingming Zha (Indiana University Bloomington); Jice Wang (UCAS); Yuhong Nan (Sun Yat-sen University); Xiaofeng Wang (Indiana Unversity Bloomington); Yuqing Zhang and Zelin Yang (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences)