Proceedings

2021

Network and Distributed System Security Symposium
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 Security

Flexsealing BGP Against Route Leaks: Peerlock Active Measurement and Analysis
   Tyler McDaniel, Jared M. Smith, Max Schuchard

A Devil of a Time: How Vulnerable is NTP to Malicious Timeservers?
   Yarin Perry, Neta Rozen-Schiff, Michael Schapira

OblivSketch: Oblivious Network Measurement as a Cloud Service
   Shangqi Lai, Xingliang Yuan, Joseph Liu, Xun Yi, Qi Li, Dongxi Liu, Nepal Surya

ROV++: Improved Deployable Defense against BGP Hijacking
   Reynaldo Morillo, Justin Furuness, Cameron Morris, James Breslin, Amir Herzberg, Bing Wang

Trust the Crowd: Wireless Witnessing to Detect Attacks on ADS-B-Based Air-Traffic Surveillance
   Kai Jansen, Liang Niu, Nian Xue, Ivan Martinovic, Christina Pöpper

Session 1B: Program Analysis 1

Towards Measuring Supply Chain Attacks on Package Managers for Interpreted Languages
   Ruiyan Duan, Omar Alrawi, Ranjita Pai Kasturi, Ryan Elder, Brendan Saltaformaggio, Wenke Lee

Processing Dangerous Paths – On Security and Privacy of the Portable Document Format
   Jens Müller, Dominik Noss, Christian Mainka, Vladislav Mladenov, Jörg Schwenk

XDA: Accurate, Robust Disassembly with Transfer Learning
   Kexin Pei, Jonas Guan, David Williams-King, Junfeng Yang, Suman Jana

Shadow Attacks: Hiding and Replacing Content in Signed PDFs
   Christian Mainka, Vladislav Mladenov, Simon Rohlmann

KUBO: Precise and Scalable Detection of User-triggerable Undefined Behavior Bugs in OS Kernel
   Changming Liu, Yaohui Chen, Long Lu
**Session 1C: Privacy**

Awakening the Web's Sleeper Agents: Misusing Service Workers for Privacy Leakage  
*Soroush Karami, Panagiotis Ilia, Jason Polakis*

All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers  
*Christoph Hagen, Christian Weinert, Christoph Sendner, Alexandra Dmitrienko, Thomas Schneider*

Improving Signal's Sealed Sender  
*Ian Martiny, Gabriel Kaptchuk, Adam Aviv, Dan Roche, Eric Wustrow*

Tales of Favicon and Caches: Persistent Tracking in Modern Browsers  
*Konstantinos Solomos, John Kristoff, Chris Kanich, Jason Polakis*

**Session 2A: Network Policies**

Reining in the Web's Inconsistencies with Site Policy  
*Stefano Calzavara, Tobias Urban, Dennis Tatang, Marius Steffens, Ben Stock*

From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration  
*Privacy under the GDPR  
Chaoyi Lu, Baojun Liu, Yiming Zhang, Zhou Li, Fenglu Zhang, Haixin Duan, Ying Liu, Joann Qiongna Chen, Jinjin Liang, Zaifeng Zhang, Shuang Hao, Min Yang*

Understanding the Growth and Security Considerations of ECS  
*Athanasiou Kountouras, Panagiotis Kintis, Athanasios Avgeidis, Thomas Papastergiou, Charles Lever, Michalis Polychronakis, Manos Antonakakis*

Mondrian: Comprehensive Inter-domain Network Zoning Architecture  
*Jonghoon Kwon, Claude Hähni, Patrick Bamert, Adrian Perrig*

**Session 2B: Program Analysis 2**

Bringing Balance to the Force: Dynamic Analysis of the Android Application Framework  
*Abdallah Dawoud, Sven Bugiel*

SymQEMU: Compilation-based symbolic execution for binaries  
*Sebastian Poeplau, Aurélien Francillon*

TASE: Reducing Latency of Symbolic Execution with Transactional Memory  
*Adam Humphries, Kartik Catting-Subramanian, Michael K. Reiter*

Refining Indirect Call Targets at the Binary Level  
*Sun Hyoung Kim, Cong Sun, Dongrui Zeng, Gang Tan*

**Session 2C: Crypto**

Obfuscated Access and Search Patterns in Searchable Encryption  
*Zhiwei Shang, Simon Oya, Andreas Peter, Florian Kerschbaum*

More than a Fair Share: Network Data Remanence Attacks against Secret Sharing-based Schemes  
*Leila Rashidi, Daniel Kostecki, Alexander James, Anthony Peterson, Majid Ghaderi, Samuel Jero, Cristina Nita-Rotaru, Hamed Okhravi, Reihaneh Safavi-Naini*
Forward and Backward Private Conjunctive Searchable Symmetric Encryption
Sikhar Patranabis, Debdeep Mukhopadhyay

Practical Non-Interactive Searchable Encryption with Forward and Backward Privacy
Shi-Feng Sun, Ron Steinfeld, Shangqi Lai, Xingliang Yuan, Amin Sakzad, Joseph Liu, Surya Nepal, Dawu Gu

Session 3A: Web Security
Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks
Mohd Sabra, Anindya Maiti, Murtuza Jadliwala

Deceptive Deletions for Protecting Withdrawn Posts on Social Media Platforms
Mohsen Minaei, S Chandra Mouli, Mainack Mondal, Bruno Ribeiro, Aniket Kate

Who's Hosting the Block Party? Studying Third-Party Blockage of CSP and SRI
Marius Steffens, Marius Musch, Martin Johns, Ben Stock

To Err.Is Human: Characterizing the Threat of Unintended URLs in Social Media
Beliz Kaleli, Brian Kondracki, Manuel Egele, Nick Nikiforakis, Gianluca Stringhini

SerialDetector: Principled and Practical Exploration of Object Injection Vulnerabilities for the Web
Mikhail Shcherbakov, Musard Balliu

Session 3B: Mobile Security
The Abuser Inside Apps: Finding the Culprit Committing Mobile Ad Fraud
Joongyum Kim, Jung-hwan Park, Sooel Son

Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks
Xianghang Mi, Siyuan Tang, Zhengyi Li, Xiaojing Liao, Feng Qian, Xiaofeng Wang

Understanding Worldwide Private Information Collection on Android
Yun Shen, Pierre-Antoine Vervier, Gianluca Stringhini

On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices
Zeyu Lei, Yuhong Nan, Yanick Fratantonio, Antonio Bianchi

Preventing and Detecting State Inference Attacks on Android
Andrea Possemato, Dario Nisi, Yanick Fratantonio

Session 3C: Blockchains
As Strong As Its Weakest Link: How to Break Blockchain DApps at RPC Service
Kai Li, Jiaqi Chen, Xianghong Liu, Yuzhe Tang, Xiaofeng Wang, Xiapu Luo

RandRunner: Distributed Randomness from Trapdoor VDFs with Strong Uniqueness
Philipp Schindler, Aljosha Judmayer, Markus Hittmeir, Nicholas Stifter, Edgar Weippl

LaKSA: A Probabilistic Proof-of-Stake Protocol
Daniel Reijsbergen, Pawel Szalachowski, Junming Ke, Zengpeng Li, Jianying Zhou
SquirRL: Automating Attack Analysis on Blockchain Incentive Mechanisms with Deep Reinforcement Learning
  Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramèr, Giulia Fanti, Ari Juels

Bitcontracts: Supporting Smart Contracts in Legacy Blockchains
  Karl Wüst, Loris Diana, Kari Kostiainen, Ghassan Karame, Sinisa Matetic, Srdjan Capkun

**Session 4A: Network Protocols**

QPEP: An Actionable Approach to Secure and Performant Broadband From Geostationary Orbit
  James Pavur, Martin Strohmeier, Vincent Lenders, Ivan Martinovic

A Formal Analysis of the FIDO UAF Protocol
  Haonan Feng, Hui Li, Xuesong Pan, Ziming Zhao

PHOENIX: Device-Centric Cellular Network Protocol Monitoring using Runtime Verification
  Mitziu Echeverria, Zeeshan Ahmed, Bincheng Wang, M. Fareed Arif, Syed Rafiul Hussain, Omar Chowdhury

The Bluetooth CYBORG: Analysis of the Full Human-Machine Passkey Entry AKE Protocol
  Michael Troncoso, Britta Hale

NetPlier: Probabilistic Network Protocol Reverse Engineering from Message Traces
  Yapeng Ye, Zhuo Zhang, Fei Wang, Xiangyu Zhang, Dongyan Xu

**Session 4B: Side-channels and Speculation**

Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel
  Zhuoran Liu, Niels Samwel, Léo Weissbart, Zhengyu Zhao, Dirk Laurent, Lejla Batina, Martha Larson

Rosita: Towards Automatic Elimination of Power-Analysis Leakage in Ciphers
  Madura A. Shelton, Niels Samwel, Lejla Batina, Francesco Regazzoni, Markus Wagner, Yuval Yarom

Hunting the Haunter — Efficient Relational Symbolic Execution for Spectre with Haunted RelSE
  Lesly-Ann Daniel, Sébastien Bardin, Tamara Rezk

SpecTaint: Speculative Taint Analysis for Discovering Spectre Gadgets
  Zhenxiao Qi, Qian Feng, Yueqiang Cheng, Mengjia Yan, Peng Li, Heng Yin, Tao Wei

**Session 4C: Malware and Cyber-crime**

Understanding and Detecting International Revenue Share Fraud
  Merve Sahin, Aurélien Francillon
Jiayun Xu, Yingjiu Li, Robert H. Deng

MINOS: A Lightweight Real-Time Cryptojacking Detection System  
Faraz Naseem, Ahmet Aris, Leonardo Babun, Ege Tekiner, A. Selcuk Uluagac

Does Every Second Count? Time-based Evolution of Malware Behavior in Sandboxes  
Alexander Küchler, Alessandro Mantovani, Yufei Han, Leyla Bilge, Davide Balzarotti

**Session 5A: “Smart” Home**

Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem  
Christopher Lentzsch, Sheel Jayesh Shah, Benjamin Andow, Martin Degeling, Anupam Das, William Enck

IoTSafe: Enforcing Safety and Security Policy with Real IoT Physical Interaction Discovery  
Wenbo Ding, Hongxin Hu, Long Cheng

PFirewall: Semantics-Aware Customizable Data Flow Control for Smart Home Privacy Protection  
Haotian Chi, Qiang Zeng, Xiaojiang Du, Lannan Luo

EarArray: Defending against DolphinAttack via Acoustic Attenuation  
Guoming Zhang, Xiaoyu Ji, Xinfeng Li, Gang Qu, Wenyuan Xu

**Session 5B: Software Defenses**

POP and PUSH: Demystifying and Defending against (Mach) Port-oriented Programming  
Min Zheng, Xiaolong Bai, Yajin Zhou, Chao Zhang, Fuping Qu

Detecting Kernel Memory Leaks in Specialized Modules with Ownership Reasoning  
Navid Emamdoost, Qiushi Wu, Kangjie Lu, Stephen McCamant

**Session 5C: Machine Learning**

Let's Stride Blindfolded in a Forest: Sublinear Multi-Client Decision Trees Evaluation  
Jack P. K. Ma, Raymond K. H. Tai, Yongjun Zhao, Sherman S.M. Chow

Practical Blind Membership Inference Attack via Differential Comparisons  
Bo Hui, Yuchen Yang, Haolin Yuan, Philippe Burlina, Neil Zhenqiang Gong, Yinzhi Cao

GALA: Greedy ComputAtion for Linear Algebra in Privacy-Preserved Neural Networks  
Qiao Zhang, Chunsheng Xin, Hongyi Wu

FARE: Enabling Fine-grained Attack Categorization under Low-quality Labeled Data  
Junjie Liang, Wenbo Guo, Tongbo Luo, Vasant Honavar, Gang Wang, Xinyu Xing
Session 6A: Fuzzing

PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles
Hyungsub Kim, Muslum Ozgur Ozmen, Antonio Bianchi, Z. Berkay Celik, Dongyan Xu

Favocado: Fuzzing Binding Code of JavaScript Engines Using Semantically Correct Test Cases
Sung Ta Dinh, Haehyun Cho, Kyle Martin, Adam Oest, Yihui Zeng, Alexandros Kapravelos, Tiffany Bao, Ruoyu Wang

WINNIE: Fuzzing Windows Applications with Harness Synthesis and Fast Cloning
Jinho Jung, Stephen Tong, Hong Hu, Jungwon Lim, Yonghwi Jin, Taesoo Kim

Reinforcement Learning-based Hierarchical Seed Scheduling for Greybox Fuzzing
Jinghan Wang, Chengyu Song, Heng Yin

Session 6B: Embedded Security

Evading Voltage-Based Intrusion Detection on Automotive CAN
Rohit Bhatia, Vireshwar Kumar, Khaled Serag, Z. Berkay Celik, Mathias Payer, Dongyan Xu

HERA: Hotpatching of Embedded Real-time Applications
Christian Niesler, Sebastian Surminski, Lucas Davi

From Library Portability to Para-rehosting: Natively Executing Microcontroller Software on Commodity Hardware
Wenqiang Li, Le Guan, Jingqiang Lin, Jiameng Shi, Fengjun Li

BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols
Eunsoo Kim, Dongkwan Kim, CheolJun Park, Insu Yun, Yongdae Kim

Session 6C: Federated Learning and Poisoning Attacks

POSEIDON: Privacy-Preserving Federated Neural Network Learning
Sinem Sav, Apostolos Pyrgelis, Juan Ramón Troncoso-Pastoriza, David Froelicher, Jean-Philippe Bossuat, Joao Sa Sousa, Jean-Pierre Hubaux

FLTrust: Byzantine-robust Federated Learning via Trust Bootstrapping
Xiaoyu Cao, Minghong Fang, Jia Liu, Neil Zhenqiang Gong

Manipulating the Byzantine: Optimizing Model Poisoning Attacks and Defenses for Federated Learning
Virat Shejwalkar, Amir Houmansadr

Data Poisoning Attacks to Deep Learning Based Recommender Systems
Hai Huang, Jiaming Mu, Neil Zhenqiang Gong, Qi Li, Bin Liu, Mingwei Xu

Session 7A: Forensics and Audits

C²SR Cybercrime Scene Reconstruction for Post-mortem Forensic Analysis
Yonghwi Kwon, Weihang Wang, Jinho Jung, Kyu Hyung Lee, Roberto Perdisci
ALchemist: Fusing Application and Audit Logs for Precise Attack Provenance without Instrumentation
   Le Yu, Shiqing Ma, Zhuo Zhang, Guanhong Tao, Xiangyu Zhang, Dongyan Xu, Vincent E. Urias, Han Wei Lin, Gabriela Ciocarlie, Vinod Yegneswaran, Ashish Gehani

WATSON: Abstracting Behaviors from Audit Logs via Aggregation of Contextual Semantics
   Jun Zeng, Zheng Leong Chua, Yinfang Chen, Kaihang Ji, Zhenkai Liang, Jian Mao

Session 7B: Trusted Computing

DOVE: A Data-Oblivious Virtual Environment
   Hyun Bin Lee, Tushar Jois, Christopher Fletcher, Carl A. Gunter

CHANCEL: Efficient Multi-client Isolation Under Adversarial Programs
   Adil Ahmad, Juhee Kim, Jaebaek Seo, Insik Shin, Pedro Fonseca, Byoungyoung Lee

Emilia: Catching Iago in Legacy Code
   Rongzhen Cui, Lianying Zhao, David Lie

Session 7C: Machine Learning Applications

CV-Inspector: Towards Automating Detection of Adblock Circumvention
   Hieu Le, Athina Markopoulou, Zubair Shafiq

FlowLens: Enabling Efficient Flow Classification for ML-based Network Security Applications
   Diogo Barradas, Nuno Santos, Luis Rodrigues, Salvatore Signorello, Fernando M. V. Ramos, André Madeira

PrivacyFlash Pro: Automating Privacy Policy Generation for Mobile Apps
   Sebastian Zimmeck, Rafael Goldstein, David Baraka

Towards Understanding and Detecting Cyberbullying in Real-world Images
   Nishant Vishwamitra, Hongxin Hu, Feng Luo, Long Cheng
Message from the General Chair

It is my pleasure to welcome you to the 2021 Network and Distributed System Security (NDSS) Symposium.

Despite going virtual this year, NDSS 2021 still offers a stellar program of leading computer security research: nearly 100 research paper presentations, six workshops, two exciting keynotes, and an emerging research poster session.

This year we have six co-located workshops split between Sunday, February 21 and Thursday, February 25, including three entirely new workshops. The workshops this year are:

1) Automotive and Autonomous Vehicle Security (AutoSec) Workshop;
2) DNS Privacy Workshop;
3) Innovative Secure IT Technologies against COVID-19 (CoronaDef) Workshop;
4) Measurements, Attacks, and Defenses for the Web (MADWeb) Workshop;
5) Learning from Authoritative Security Experiment Results (LASER) Workshop; and
6) Binary Analysis Research (BAR) Workshop.

I'd like to thank Yasemin Acar and Bradley Reaves, the Workshops Co-Chairs, and Karen O'Donoghue, Steering Group Co-Chair, for bringing together such an exciting set of workshops.

Building on recent successes, this year we're continuing the tradition of organizing a poster session to showcase both in-progress and exciting recent work in various aspects of computer security. Thanks are due to Xiaojing Liao and Adwait Nadkarni, the Poster Session Co-Chairs, for making sure we have an excellent poster program.

For NDSS 2021, we have continued the revised submission model, which includes two submission phases and ensures that all papers submitted to either of these two phases are processed in time to appear in the NDSS 2021 proceedings. I'd like to thank Program Committee Co-Chairs Ahmad-Reza Sadeghi and Farinaz Koushanfar for their efforts for enabling NDSS 2021 to meet the goals of this submission model. Also, I thank the program committee members and external reviewers whose efforts enable NDSS 2021 to develop an excellent program in a timely fashion.

Many individuals have contributed to making NDSS 2021 a success in this virtual environment, including everyone on the Steering Group, Organizing Committee, Award Committees, and the Internet Society and Association Management Solutions staff. I'd like to thank all of them for their tireless efforts in making NDSS a great event!

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, Google, IBM, Intel Security, Microsoft Research, National Science Foundation, Novi, Palo Alto Networks, and Qualcomm. I also thank the Internet Society additionally for hosting the symposium and once again providing funds for our student grants.

Finally, thank you for participating in the symposium and contributing to making NDSS a success. I wish you all an excellent NDSS 2021!

Trent Jaeger
General Chair, NDSS 2021
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 Symposium (NDSS) 2021, held virtually on February 21-25, 2021. For the past 28 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 573 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 two-day online program committee meeting on October 19-20, 2020. At the end of the review process, 87 papers (15.2% 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 2021. General Chair Trent Jaeger 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 Salsaformaggio 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 two-day single-track schedule with success. Our special thanks also go to Tommaso Frassetto and Patrick Jauernig from TU Darmstadt for their 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 as well as the specialized PC members who were added to the PC to help out during the review process due to the high number of submissions 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 2021 and all attendees who are virtually joining us at NDSS 2021, without whom NDSS would not be possible. Enjoy the conference!

Ahmad-Reza Sadeghi and Farinaz Koushanfar
Program Co-Chairs, NDSS 2021
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 28 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 2021 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.

Due to the events of 2020, NDSS 2021 will be the first ever virtual NDSS symposium. While I hope that you will all be able to meet face-to-face again in 2022, the program committee and event organization team has put together an exceptional agenda for the online symposium. This agenda is a full five days including six workshops, 90 paper presentations, two exciting keynotes, 19 posters for the Poster Session, and a virtual hallway track for networking and collaboration. The two keynotes this year are particularly important and timely topics. Dr. Diana L. Burley, Vice Provost for Research at American University (AU), will open the symposium with a discussion of Diversity, Equity, Inclusion, and Integrity. On Tuesday, Gavin O’Gorman will talk about the recent Solar Winds attack.

NDSS 2021 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 Trent Jaeger, Shadow General Chair Carrie Gates, Program Committee Co-chairs Ahmad-Reza Sadeghi and Farinaz Koushanfar, 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 sponsor Google; our Silver sponsors ByteDance, IBM, Intel Security, Microsoft Research, Palo Alto Networks, and Qualcomm; our Bronze sponsors Novi and Checkpoint; and our Supporting sponsor Baidu.

On behalf of the Internet Society, I welcome you to NDSS 2021. I hope you have an enjoyable and productive week.

Andrew Sullivan
CEO, Internet Society
Program Committee

Ahmad-Reza Sadeghi, Technische Universität Darmstadt (Program Co-Chair)
Farinaz Koushanfar, University of California, San Diego (Program Co-Chair)

Benjamin Andow, Google
Cornelius Aschermann, Oracle
Tiffany Bao, Arizona State University
Adam Bates, University of Illinois
Lejla Batina, Radboud University
Lujo Bauer, Carnegie Mellon University
Antonio Bianchi, Purdue University
Jeremiah Blocki, Purdue University
Kevin Butler, University of Florida
Rosario Cammarota, Intel AI Research
Srdjan Capkun, ETH Zurich
Yingying Chen, Rutgers University
Anupam Das, North Carolina State University
Lucas Davi, University of Duisburg-Essen
Alexandra Dmitrienko, University of Wuerzburg
Brendan Dolan-Gavitt, NYU
Adam Doupe, Arizona State University
Manuel Egele, Boston University
William Enck, North Carolina State University
Sebastian Faust, TU Darmstadt
Marc Fischlin, TU Darmstadt
Aurélien Francillon, EURECOM
Carrie Gates, Bank of America
Xinyang Ge, Microsoft Research
Neil Gong, Duke University
Guofei Gu, Texas A&M
Kevin Hamlen, University of Texas at Dallas
Amir Houmansadr, UMass Amherst
Hsu-Chun Hsiao, National Taiwan University
Trent Jaeger, Pennsylvania State University
Suman Jana, Columbia University
Samuel Jero, MIT Lincoln Laboratory
Limin Jia, CMU
Yier Jin, University of Florida
Brent ByungHoon Kang, KAIST
Yongdae Kim, KAIST
Sam King, UC Davis
Engin Kirda, Northeastern University
Katharina Kohls, Ruhr-University Bochum
Per Larsen, UC Irvine and Immunant, Inc.
Qi Li, Tsinghua University
We thank the following members of the “Specialized PC” who strongly supported us with their expertise in the NDSS review process:

Alessandra Scafuro, North Carolina State
Arthur Gervais, Imperial College London
    Aysajan Abidin, KU Leuven
    Bart Preneel, KU Leuven
Joel Frank, Ruhr-Universität Bochum
Kapil Singh, IBM T.J. Watson Research Center
    Pedro Moreno-Sanchez, TU Wien
    Ren Zhang, Nervos
Sazzadur Rahaman, University of Arizona
    Shouling Ji, Zhejiang University
    Srinath Setty, Microsoft Research
Ting Chen, University of Electronic Science and Technology of China
    Xiapu Luo, The Hong Kong Polytechnic University
**External Reviewers**

Abbas Acar, *Florida International University*
Abhishek Bichhawat, *Carnegie Mellon University*
Ágnes Kiss, *CISPA Helmholtz Center for Information Security*
Ahmet Aris, *Florida International University*
Akash Madhusudan, *KU Leuven*
Akul Goyal, *University of Illinois*
Ala' Darabseh, *New York University Abu Dhabi*
Alejandro Mera, *Northeastern University*
Alex Block, *Purdue University*
Alexander Bulekov, *Boston University*
Amirhossein Ghafari, *UMass Amherst*
Amit Kumar Sikder, *Georgia Institute of Technology*
Amit Seal Ami, *William & Mary*
Aysajan Abidin, *KU Leuven*
Baojun Liu, *Tsinghua University*
Ben Harsha, *Purdue University*
Bo Feng, *Northeastern University*
Camille Cobb, *Carnegie Mellon University*
Chen Yan, *Zhejiang University*
Deliang Chang, *Tsinghua University*
Dohyun Kim, *KAIST*
Daniele Cozzo, *KU Leuven*
David Paaßen, *University of Duisburg-Essen*
Deliang Chang, *Tsinghua University*
Dohyun Kim, *KAIST*
Eunsoo Kim, *KAIST*
Evangelos Bitsikas, *New York University Abu Dhabi*
Faysal Hossain Shezan, *University of Virginia*
Feiyang Qiu, *KU Leuven*
Fengting Li, *Tsinghua University*
Fnu Suya, *University of Virginia*
Geonwoo Kim, *KAIST*
Guangliang Yang, *Georgia Tech*
Hadi Abdullah, *University of Florida*
Helen Möllering, *TU Darmstadt*
Hongil Kim, *Qualcomm*
Hossein Yalame, *TU Darmstadt*
Hsuan-Chi (Austin) Kuo, University of Illinois Urbana-Champaign
Hunter Searle, University of Florida
Insu Yun, KAIST
Jaehoon Kim, KAIST
James K. Howes IV, University of Florida
Jason Liu, University of Illinois
Jiacen Xu, University of California, Irvine
Jiaming Mu, Tsinghua University
Jian Mao, Beihang University
Jianfeng Chi, University of Virginia
Jim Howes, University of Florida
Jiyong Yu, University of Illinois Urbana-Champaign
Jiyo ng Yu, University of Illinois Urbana-Champaign
Jo Vliegen, KU Leuven
Joann Qiongna Chen, University of California, Irvine
JoonHa Jang, KAIST
Juhwan Noh, NSR
Jun Ho Huh, Samsung
Jun Zeng, National University of Singapore
Kaihang Ji, National University of Singapore
Kaushal Kafle, William & Mary
Kevin Hong, Texas A&M University
Kevin Warren, University of Florida
Laurens Le Jeune, KU Leuven
Leonardo Babun, Johns Hopkins University Applied Physics Lab
Liang Niu, New York University Abu Dhabi
Logan Blue, University of Florida
Luis Vargas, University of Florida
Mangi Cho, KAIST
Marco Holz, TU Darmstadt
Marius Steffens, CISPA Helmholtz Center for Information Security
Martijn de Vos, TU Delft
Mathy Vanhoef, New York University Abu Dhabi
Matt Jones, Google
Matthew McNiece, North Carolina State University
Md Masoom Rabbani, KU Leuven
Menghao Zhang, Tsinghua University
Michael Rodler, University of Duisburg-Essen
Milad Nasr, UMass Amherst
Mincheol Son, KAIST
Minjoon Park, KAIST
Min Suk Kang, KAIST
Mohammad Hassan Ameri, Purdue University
Muhammad Adil Inam, University of Illinois
Muhammad Shujaat Mirza, New York University Abu Dhabi
Muoi Tran, National University of Singapore
Nian Xue, New York University Abu Dhabi
Oguzhan Ersoy, TU Delft
Oleksandr Tkachenko, TU Darmstadt
Peiyang Li, Tsinghua University
Peiyuan Liu, Purdue University
Pubali Datta, University of Illinois
Qilei Yin, Tsinghua University
Qixiao Lin, Beihang University
Raine Nieminen, TU Darmstadt
Raj Vardhan, Texas A&M University
Raluca-Georgia Diugan, New York University Abu Dhabi
Reza Mirzazade, Northeastern University
Riccardo Paccagnella, University of Illinois
Ruimin Sun, Northeastern University
Ruoyu Wu, Purdue University
Sangwook Bae, KAIST
Sathvik Prasad, North Carolina State University
Satwik Pradhu Kumble, TU Delft
Sebastian Roth, CISPA Helmholtz Center for Information Security
Sebastian Surminski, University of Duisburg-Essen
Seungwon Shin, Samsung
Song Min Kim, KAIST
Soobin Lee, NSR
Suyeon Yoo, KAIST
Taekkyung Oh, KAIST
Tamjid Al Rahat, University of Virginia
Tianhao Wang, Purdue University
Tobias Cloosters, University of Duisburg-Essen
Tu Le, University of Virginia
Tyler Tucker, University of Florida
Vanessa Frost, University of Florida
Varun Madathil, North Carolina State University
Virat Shejwalkar, UMass Amherst
Washington Garcia, University of Florida
Weidong Zhu, University of Florida
William Blair, Boston University
Wuwai Zhang, Purdue University
Xiaoyu Ji, Zhejiang University
Yangyong Zhang, Texas A&M University
Yanjiao Chen, Zhejiang University
Yinfang Chen, National University of Singapore
Yujin Kwon, KAIST
Yunpeng Liu, Tsinghua University
Yushi Cheng, Zhejiang University
Zhe Zhou, Fudan University
Zhichuang Sun, Northeastern University
Zijie Yang, Tsinghua University
Ziqi Yang, Zhejiang University
Organizing Committee

General Chair
Trent Jaeger
Pennsylvania State University

Shadow General Chair
Carrie Gates
Bank of America

Program Co-Chairs
Ahmad-Reza Sadeghi
Technische Universität Darmstadt

Farninaz Koushanfar
University of California, San Diego

Workshops Co-Chairs
Brad Reaves
North Carolina State University

Yasemin Acar
Leibniz University Hannover

Poster Session Co-Chairs
Adwait Nadkarni
College of William & Mary

Xiaojing Liao
Indiana University

Student Support Committee
Alexandra Dmitrienko (Chair)
University of Würzburg

Zhiyun Qian
UC Riverside

Limin Jia
Carnegie Mellon University

Stefanie Roos
TU Delft

Nele Mentens
KU Leuven

Elizabeth Stolbert
Carleton University

Publicity Chair
Brendan Saltaformaggio
Georgia Institute of Technology

Historian and Publications Chair
David Balenson
SRI International
Sponsorship Chair
Robert Broberg
Nanoglass Photonics

Past General Chair
Lujo Bauer
Carnegie Mellon University

Local Arrangements Chair
Thomas Hutton
San Diego Supercomputer Center

Event Manager
Karen O'Donoghue
Internet Society
Steering Group

Co-Chairs

Trent Jaeger  
Pennsylvania State University

Karen O'Donoghue  
Internet Society

Steering Group Members

David Balenson  
SRI International

Ari Juels  
Cornell University

Lujo Bauer  
Carnegie Mellon University

Farinaz Koushanfar  
University of California, San Diego

Srdjan Capkun  
ETH Zurich

Zhenkai Liang  
National University of Singapore

Gabriela Ciocarlie  
Elpha Secure

Sarah Meiklejohn  
University College London

Carrie Gates  
Bank of America

Alina Oprea  
RSA Laboratories

Tom Hutton  
San Diego Supercomputer Center

Dongyan Xu  
Purdue University