Proceedings

2017

Network and Distributed System Security Symposium
Table of Contents

General Chair’s Message
Program Chair’s Message
Organizing Committee
Program Committee
Steering Group

Keynote Speaker: J. Alex Halderman, Professor, University of Michigan

Session 1: Applied Crypto and Cryptocurrencies

IO-DSSE: Scaling Dynamic Searchable Encryption to Millions of Indexes By Improving Locality
   I. Miers, P. Mohassel

ObliviSync: Practical Oblivious File Backup and Synchronization
   A.J. Aviv, S. Geol Choi, T. Mayberry, D.S. Roche

TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub
   E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, S. Goldberg

P2P Mixing and Unlinkable Bitcoin Transactions
   T. Ruffing, P. Moreno-Sanchez, A. Kate

SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks
   G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei

Session 2A: Virtualization and SDN

DELTA: A Security Assessment Framework for Software-Defined Networks
   S. Lee, C. Yoon, C. Lee, S. Shin, V. Yegneswaran, P. Porras

PSI: Precise Security Instrumentation for Enterprise Networks
   T. Yu, S. K. Fayaz, M. Collins, V. Sekar, S. Seshan

On the Safety and Efficiency of Virtual Firewall Elasticity Control
   J. Deng, H. Li, H. Hu, K.-C. Wang, G.-J. Ahn, Z. Zhao, W. Han

Deconstructing Xen
   L. Shi, Y. Wu, Y. Xia, N. Dautenhahn, H. Chen, B. Zang, H. Guan, J. Li
**Session 2B: Web Security**

**Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web**  
* T. Lauinger, A. Chaabane, S. Arshad, W. Robertson, C. Wilson, E. Kirda

**Enabling Reconstruction of Attacks on Users via Efficient Browsing Snapshots**  
* P. Vadrevu, J. Liu, B. Li, B. Rahbarinia, K. H. Lee, R. Perdisci

**(Cross-)Browser Fingerprinting via OS and Hardware Level Features**  
* Y. Cao, S. Li, E. Wijmans

**Fake Co-visititation Injection Attacks to Recommender Systems**  
* G. Yang, N. Z. Gong, Y. Cai

**Session 3A: User Authentication**

**Broken Hearted: How To Attack ECG Biometrics**  
* S. Eberz, N. Paoletti, M. Roeschlin, A. Patané, M. Kwiatkowska, I. Martinovic

**Towards Implicit Visual Memory-Based Authentication**  
* C. Castelluccia, M. Dürmuth, M. Golla, F. Deniz

**KEH-Gait: Towards a Mobile Healthcare User Authentication System by Kinetic Energy Harvesting**  
* W. Xu, G. Lan, Q. Lin, S. Khalifa, N. Bergmann, M. Hassan, W. Hu

**A Large-scale Analysis of the Mnemonic Password Advice**  
* J. Kiesel, B. Stein, S. Lucks

**Cracking Android Pattern Lock in Five Attempts**  

**Session 3B: Malware**

**Dial One for Scam: A Large-Scale Analysis of Technical Support Scams**  
* N. Miramirkhani, O. Starov, N. Nikiforakis

**Automated Synthesis of Semantic Malware Signatures using Maximum Satisfiability**  
* Y. Feng, O. Bastani

**MAMADROID: Detecting Android Malware by Building Markov Chains of Behavioral Models**  
* E. Mariconti, L. Onwuzurike, P. Andriotis, E. De Cristofaro, G. Ross, G. Stringhini

**A Broad View of the Ecosystem of Socially Engineered Exploit Documents**  
* S. Le Blond, C. Gilbert, U. Upadhyay, M. Gomez Rodriguez, D. Choffnes
Catching Worms, Trojan Horses and PUPs: Unsupervised Detection of Silent Delivery Campaigns
B. J. Kwon, V. Srinivas, A. Deshpande, T. Dumitras

Session 4A: TLS et al.

Measuring small subgroup attacks against Diffie-Hellman
L. Valenta, D. Adrian, A. Sanso, S. Cohney, J. Fried, M. Hastings,
J. A. Halderman, N. Heninger

Indiscreet Logs: Persistent Diffie-Hellman Backdoors in TLS
K. Dorey, N. Chang-Fong, A. Essex

WireGuard: Next Generation Kernal Network Tunnel
J. A. Donenfeld

The Security Impact of HTTPS Interception
Z. Durumeric, Z. Ma, D. Springall, R. Barnes, N. Sullivan, E. Bursztein, M. Bailey
J. A. Halderman, V. Paxson

Session 4B: Secure Computation

Fast Actively Secure OT Extension for Short Secrets
A. Patra, P. Sarkar, A. Suresh

Constant Round Maliciously Secure 2PC with Function-independent Preprocessing using LEGO
J. B. Nielsen, T. Schneider, R. Trifiletti

Pushing the Communication Barrier in Secure Computation using Lookup Tables
G. Dessouky, F. Koushanfar, A.-R. Sadeghi, T. Schneider, S. Zeitouni,
M. Zohner

Using Fully Homomorphic Encryption for Statistical Analysis of Categorical, Ordinal and Numerical Data
W. Lu, S. Kawasaki, J. Sakuma

Session 5A: Mobile Privacy and Security

Dark Hazard; Learning-based, Large-scale Discovery of Hidden Sensitive Operations in Android Apps
X. Pan, X. Wang, Y. Duan, X.F. Wang, H. Yin

Show Me the Money! Finding Flawed Implementations of Third-party In-app Payment in Android Apps
W. Yang, Y. Zhang, J. Li, H. Liu, Q. Wang, Y. Zhang, D. Gu
WindowGuard: Systematic Protection of GUI Security in Android  
C. Ren, P. Liu, S. Zhu

Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis  
A. Continella, Y. Fratantonio, M. Lindorfer, A. Puccetti, A. Zand, C. Kruegel, G. Vigna

Automated Analysis of Privacy Requirements for Mobile Apps  
S. M. Bellovin, J. Reidenberg

Session 5B: Software and System Security (Part 1)

Dachshund: Digging for and Securing Against (Non-)Blinded Constants in JIT Code  
G. Maisuradze, M. Backes, C. Rossow

Safelnit: Comprehensive and Practical Mitigation of Uninitialized Read Vulnerabilities  
A. Milburn, H. Bos, C. Giuffrida

MARX: Uncovering Class Hierarchies in C++ Programs  
A. Pawlowski, M. Contag, V. van der Veen, C. Ouwehand, T. Holz, H. Bos,  
E. Athanasopoulos, C. Giuffrida

PT-Rand: Practical Mitigation of Data-only Attacks against Page Tables  

Dynamic Virtual Address Range Adjustment for Intra-Level Privilege Separation on ARM  
Y. Cho, D. Kwon, H. Yi, Y. Paek

Session 6A: Cloud and Potpourri

Hello from the Other Side: SSH over Robust Cache Covert Channels in the Cloud  
C. Maurice, M. Weber, M. Schwarz, L. Giner, D. Gruss, C. A. Boano,  
S. Mangard, K. Römer

Dynamic Differential Location Privacy with Personalized Error Bounds  
L. Yu, L. Liu, C. Pu

Are We There Yet? On RPKI’s Deployment and Security  
Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, H. Shulman

TenantGuard: Scalable Runtime Verification of Cloud-Wide VM-Level Network Isolation  
Y. Wang, T. Madi, S. Majumdar, Y. Jarraya, A. Alimohammadiifar, M. Pourzandi  
L. Wang, M. Debbabi
Session 6B: Tor

Dissecting Tor Bridges: A Security Evaluation of their Private and Public Infrastructures
  S. Matic, C. Troncoso, J. Caballero

The Effect of DNS on Tor's Anonymity
  B. Greschbach, T. Pulls, L.M. Roberts, P. Winter, N. Feamster

Avoiding The Man on the Wire: Improving Tor's Security with Trust-Aware Path Selection
  A. Johnson, R. Jansen, A. D. Jaggard, J. Feigenbaum, P. Syverson

HisTorɛ: Differentially Private and Robust Statistics Collection for Tor
  A. Mani, M. Sherr

Session 7: Trusted Execution Environments

SGX-Shield: Enabling Address Space Layout Randomization for SGX Programs
  J. Seo, B. Lee, S. Kim, M.-W. Shih, I. Shin, D. Han, T. Kim

T-SGX: Eradicating Controlled-Channel Attacks Against Enclave Programs
  M.-W. Shih, S. Lee, T. Kim, M. Peinado

BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments
  A. Machiry, E. Gustafson, C. Spensky, C. Salls, N. Stephens, R. Wang,
  A. Bianchi, Y. R. Choe, C. Kruegel, G. Vigna

HOP: Hardware makes Obfuscation Practical
  K. Nayak, C.W. Fletcher, L. Ren, N. Chandran, S. Lokam, E. Shi, V. Goyal

PANOPLY: Low-TCB Linux Applications With SGX Enclaves
  S. Shinde, D. L. Tien, S. Tople, P. Saxena

Keynote Speaker: Trent Adams, Director of Information Security, PayPal

Session 8: Cyberphysical Security

Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit
  L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. Mohammed,
  S.A. Zonouz

ContexloT: Towards Providing Contextual Integrity to Appified IoT Platforms
  Y.J. Jia, Q.A. Chen, S.i Wang, A. Rahmati, E. Fernandes, Z.M. Mao,
  A. Prakash
FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild
  Z. Li, W. Wang, C. Wilson, J. Chen, C. Qian, T. Jung, L. Zhang, K. Liu,
  X. Li, Y. Liu

Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis
  C. Fachkha, E. Bou-Harb, A. Keliris, N. Memon, M. Ahamad

Wi-Fly? : Detecting Privacy Invasion Attacks by Consumer Drones
  S. Birnbach, R. Baker, I. Martinovic

Session 9: Attacks

ASLR on the Line: Practical Cache Attacks on the MMU
  B. Gras, K. Razavi, E. Bosman, H. Box, C. Giuffrida

Unleashing Use-Before-Initialization Vulnerabilities in the Linux Kernel Using Targeted Stack Spraying

Address-Oblivious Code Reuse: On the Effectiveness of Leakage-Resilient Diversity

An Evil Copy: How the Loader Betrays You
  X. Ge, M. Payer, T. Jaeger

Session 10: Software and System Security (Part II)

Stack Bounds Protection with Low Fat Pointers
  G.J. Duck, R. H. C. Yap, L. Cavallaro

VUzzer: Application-aware Evolutionary Fuzzing
  S. Rawat, V. Jain, A. Kumar, L. Cojocar, C. Giuffrida, H. Bos

Self Destructing Exploit Executions via Input Perturbation
  Y. Kwon, B. Saltaformaggio, I L. Kim, K. H. Lee, X. Zhang, D. Xu

A Call to ARMs: Understanding the Costs and Benefits of JIT Spraying Mitigations
  W. Lian, H. Shacham, S. Savage

Ramblr: Making Reassembly Great Again
  R. Wang, Y. Shoshitaishvili, A. Bianchi, A. Machiry, J. Grosen, P. Grosen,
  C. Kruegel, G. Vigna
General Chair’s Message

It is my pleasure to welcome you to the 24th Annual Network and Distributed System Security Symposium.

This year we have two collocated workshops: DNS Privacy Workshop and Usable Security (USEC) Workshop. The workshops encompass two critical topics in network and distributed systems security, privacy and usability. I'd like to thank Matthew Smith, the Workshop Chair, and Karen O'Donoghue, Steering Group Co-Chair, for bringing together such an exciting pair of workshops.

Building on recent success, 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 Johanna Amann and Amir Houmansadr, the Poster Co-Chairs, for making sure we have an excellent poster program.

Due to increased interest in our field and in NDSS, more papers will be presented at NDSS this year than in any past year, yielding a particularly rich and exciting program. Selecting the papers is a task that involves many people and many hours of hard work. I'd like to thank Ari Juels, the Program Chair, as well Patrick Traynor, Shadow Program Chair, for the tremendous amount of work they donated and the excellent job they've done in putting together this year's program.

Many individuals have contributed to making NDSS a success, including everyone on the Steering Group, Organizing Committee, and the Internet Society and Association Management Solutions staff. I’d like thank all of them for contributing their time and effort.

NDSS is possible in large part thanks to our generous sponsors. I'd like to thank Baidu, Cisco, Afilias, Check Point Software Technologies, Qualcomm, San Diego Supercomputer Center, and Salesforce for their support, and the Internet Society for hosting the symposium. Funds for our student grants were provided by the National Science Foundation and the Internet Society.

Finally, thank you, all, for participating in the symposium and through that adding the key ingredient that makes NDSS a success. I wish you all an excellent 24th NDSS!

Lujo Bauer
General Chair, NDSS’17
Carnegie Mellon University
Program Chair's Message

It is my great pleasure to welcome you to the 24th Annual Network & Distributed System Security Symposium (NDSS 2017), held at the Catamaran Resort Hotel and Spa in San Diego, CA, United States from February 26 - March 1, 2017. NDSS fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of network and distributed systems security technologies.

This year NDSS received a record 423 valid 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. Papers went through three rounds of review. Reviewing culminated in a one-day in-person program committee meeting, at which 68 papers (approximately 16%) were selected to appear in the program.

Organizing a conference as large as NDSS is a substantial endeavor, and I'd like to extend my sincere thanks to everyone who contributed her or his time and effort. I'd also like to specifically thank a few individuals who made particular contributions to NDSS 2017. Karen O'Donoghue and Julie Rowland-Lane handled most of the logistics of organizing the conference, as well as shepherding a new program chair. Patrick Traynor served as the shadow chair; my job was made easier by his being there to catch oversights. Yier Jin graciously hosted the PC meeting at the University of Central Florida in Orlando. This year we tried an experiment in which we ran the PC meeting in two parallel tracks. Several students were especially helpful in addressing the logistical challenges this experiment involved. I'd like to thank Fan Zhang for his extensive technical support, Grant Hernandez and Bradley Reaves for their assistance on the ground, and Yan Ji for creating a scheduling tool for the meeting. Thanks also to David Balenson, the Publications Chair, for his efforts and persistence in producing the proceedings you have before you. I'd also like to thank everyone who served on the program committee and put in the time both to review papers and travel to the PC meeting. It was my pleasure and honor to have worked with you to put together the program for NDSS 2017. Also crucial to the success of NDSS are the authors who submitted papers and the attendees, without whom NDSS would not be possible. Welcome to NDSS 2017. I hope you find the program informative and stimulating.

Ari Juels
Cornell Tech
Program Chair, NDSS'17
Program Committee

Ari Juels, Cornell Tech (Program Chair)
Patrick Traynor, University of Florida (Shadow Program Chair)

Johanna Amann, ICSI
Manos Antonakakis, Georgia Institute of Technology
Erman Ayday, Bilkent University
Davide Balzarotti, EURECOM
David Barrera, ETH Zurich
Adam Bates, University of Illinois Urbana Champaign (UIUC)
Lujo Bauer, Carnegie Mellon University
Alex Biryukov, University of Luxembourg
Kevin Butler, University of Florida
Nicolas Christin, Carnegie Mellon University
Dana Dachman-Soled, University of Maryland
Anupam Datta, Carnegie Mellon University
Emiliano De Cristofaro, University College London
Tudor Dumitras, University of Maryland
Manuel Egele, Boston University
William Enck, North Carolina State University
David Evans, University of Virginia
Ittay Eyal, Cornell University
Domenic Forte, University of Florida
Aurelien Francillon, EURECOM
Matthew Fredrikson, Carnegie Mellon University
Guofei Gu, Texas A&M University
Alex Halderman, University of Michigan
Amir Herzberg, Bar Ilan University
Amir Houmansadr, University of Massachusetts Amherst
Yier Jin, UCF
Jaeyeon Jung, Microsoft Research
Yongdae Kim, KAIST
Engin Kirda, Northeastern University
Farinaz Koushanfar, UCSD
Ralf Kuesters, University of Trier
Wenke Lee, Georgia Institute of Technology
Zhenkai Liang, National University of Singapore
Ben Livshits, Microsoft Research
Long Lu, Stony Brook University
Ivan Martinovic, Oxford University
Jonathan McCune, Google
Patrick McDaniel, Pennsylvania State University
Sarah Meiklejohn, University College London
Andrew Miller, UMD / UIUC
Prateek Mittal, Princeton University
Muhammad Naveed, USC
Steven Murdoch, University College London
Steven Myers, Indiana University Bloomington
Alina Oprea, Northeastern University
Charalampos Papamanthou, University of Maryland
Chunyi Peng, The Ohio State University
Christina Poepper, New York University Abu Dhabi
Raluca Popa, University of California, Berkeley
Mike Reiter, UNC Chapel Hill
Will Robertson, Northeastern University
Ahmad-Reza Sadeghi, TU Darmstadt
Vyas Sekar, CMU
abhi shelat, University of Virginia
Reza Shokri, Cornell Tech
Tom Shrimpton, University of Florida
Ed Suh, Cornell University
Stefano Tessaro, UCSB
Nikos Triandopoulos, Boston University
Venkat Venkatakrishnan, University of Illinois Chicago
XiaoFeng Wang, Indiana University Bloomington
Dongyan Xu, Purdue University
Yinqian Zhang, The Ohio State University
Organizing Committee

General Chair
Lujo Bauer
Carnegie Mellon University

Program Chair
Ari Juels
Cornell Tech

Shadow Program Chair
Patrick Traynor
University of Florida

Local Arrangements Chair
Thomas Hutton
San Diego Supercomputer Center
University of California, San Diego

Publications Chair
David Balenson
SRI International

Workshops Chair
Matthew Smith
Rheinische Friedrich-Wilhelms-Universität Bonn

Poster Co-Chairs
Johanna Amann
International Computer Science Institute

Amir Houmansadr
University of Massachusetts Amherst

Event Manager
Karen O'Donoghue
Internet Society

Event Coordinator
Julie Rowland
Association Management Solutions
Steering Group

Co-Chairs

Lujo Bauer
Carnegie Mellon University

Karen O’Donoghue
Internet Society

Steering Group Members

David Balenson
SRI International

Farinaz Koushanfar
University of California San Diego

Davide Balzarotti
EURECOM Graduate School and Research Center

Alina Oprea
RSA Laboratories

Tom Hutton
San Diego Supercomputer Center

Deborah Shands
Aerospace Corporation

Yongdae Kim
Korea Advanced Institute of Science and Technology

Paul Syverson
Naval Research Lab

Doug Szajda
University of Richmond