October 24–28, 2016
Vienna, Austria

Association for Computing Machinery

Advancing Computing as a Science & Profession

CCS'16

Proceedings of the 2016 ACM SIGSAC Conference on

Computer and Communications Security

Sponsored by:

ACM SIGSAC

Supported by:

National Science Foundation, SBA Research, CISCO, Huawei, Baidu, IBM Research, Office of Naval Research, Hewlett-Packard Enterprise, Bosch, Google, SAP, and Cyan Security Group

Association for
Computing Machinery

Advancing Computing as a Science & Profession

The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York, New York 10121-0701

Copyright © 2016 by the Association for Computing Machinery, Inc. (ACM). Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from: permissions@acm.org or Fax +1 (212) 869-0481.

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through www.copyright.com.

Notice to Past Authors of ACM-Published Articles

ACM intends to create a complete electronic archive of all articles and/or other material previously published by ACM. If you have written a work that has been previously published by ACM in any journal or conference proceedings prior to 1978, or any SIG Newsletter at any time, and you do NOT want this work to appear in the ACM Digital Library, please inform permissions@acm.org, stating the title of the work, the author(s), and where and when published.

ISBN: 978-1-4503-4139-4

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 30777
New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)
+1-212-626-0500 (Global)
Fax: +1-212-944-1318
E-mail: acmhelp@acm.org
Hours of Operation: 8:30 am – 4:30 pm ET

Printed in the USA .

CCS 2016 General Chair’s Welcome

It is our great pleasure to welcome you to the 2016 ACM Conference on Computer and Communications Security. CCS is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery. CCS brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. It provides an environment to conduct intellectual discussions. From its inception, CCS has established itself as a high standard research conference in its area. Its reputation continues to grow and is reflected in the prestigious technical program.

We are proud to say that CCS 2016 is the largest CCS conference ever. From 2002 to 2015, the number of submission rose from roughly 150 to 660. This year, CCS received the record number of 831 submissions. Together with 13 workshops, 7 tutorials, two prestigious keynotes by Martin Hellman and Ross Anderson, a panel and various industrial talks, CCS 2016 probably is the largest scientific event in the area of information security.

CCS 2016 would not have been possible without the help of numerous volunteers. We first want to thank all authors who have submitted their work to CCS – without their commitment CCS 2016 would never have been possible. We furthermore want to thank the Program Committee, who diligently supported the peer review process and selected an interesting program. Finally, we want to thank the Program Chairs and the entire Organization Committee for their dedication and commitment. Special thanks go to Yvonne Poul for her wonderful handling of the organization.

We hope that you will find this program interesting and thought-provoking and that the conference will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world.

Stefan Katzenbeisser
CCS 2016 General co-Chair
TU Darmstadt, Germany

Edgar Weippl
CCS 2016 General co-Chair
SBA Research, Austria

CCS 2016 Program Chairs' Welcome

It is our pleasure to present the proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS 2016), held in Vienna, Austria, on October 24–28, 2016. All papers in the proceedings were subject to a rigorous process of peer review. We received 831 fully reviewed submissions, the largest number of submissions received to date by a computer security conference. A Program Committee comprising 141 experts from 20 countries, helped by 360 external reviewers, evaluated these submissions, employing the customary double-blind review procedure. The review process had a 16.5% acceptance rate, resulting in 137 papers being accepted to the program, and very broad coverage of the entire security area.

The review process was organized in three phases. In the first review round, at least two preliminary reviews were written for each paper. Most papers went on to a second round, during which at least one additional review was solicited. At this point, the authors were given an opportunity to respond to the comments received (in a rebuttal phase). Finally, in the third round, the program committee actively and comprehensively discussed the papers, and, if necessary, requested additional reviews. Within the program committee, a "rebuttal committee" subgroup helped to spur discussion, to ensure that author responses were considered carefully, and to reflect the post-review discussion in the feedback to authors. New this year, we relied heavily on the TPMS system for assigning submissions to reviews, and we thank Laurent Charlin for writing this system and for all his help with using it.

We are profoundly grateful to the members of the Program Committee for their hard work, professionalism, and responsiveness under very tight deadline requirements. On average, PC members reviewed 17 papers. We are also indebted to the external reviewers whose focused expertise added substantial value to the feedback for authors. Moreover, we want to thank the CCS 2016 conference committee: the general chairs, workshop, poster, and tutorial co-chairs, and other chairs and organizers, as well as the steering committee, for their advice on how to produce a strong program and for their help with these proceedings. Finally, we thank the authors of all submitted papers and all attendees for their participation in the technical discussion during the conference. We hope that you find the program stimulating and helpful in advancing the exciting area of computer and communications security.

Shai Halevi	**Christopher Kruegel**	**Andrew Myers**
CCS'16 Program Co-Chair	*CCS'16 Program Co-Chair*	*CCS'16 Program Co-Chair*
IBM Research, USA	*UC Santa Barbara, USA*	*Cornell University, USA*

Table of Contents

CCS 2016 Conference Organization xxiii

CCS 2016 Sponsors & Supporters xxxii

Keynote

- **Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic** 1
  Martin E. Hellman *(Stanford University)*

Paper Session 1A: Blockchain I

- **On the Security and Performance of Proof of Work Blockchains** 3
  Arthur Gervais *(ETH Zurich)*, Ghassan O. Karame *(NEC Laboratories)*,
  Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, Srdjan Čapkun *(ETH Zurich)*
- **A Secure Sharding Protocol for Open Blockchains** 17
  Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, Prateek Saxena
  (National University of Singapore)
- **The Honey Badger of BFT Protocols** 31
  Andrew Miller *(University of Illinois at Urbana-Champaign)*, Yu Xia *(Massachusetts Institute of Technology)*,
  Kyle Croman, Elaine Shi *(Cornell University)*, Dawn Song *(University of California, Berkeley)*

Paper Session 1B: Differential Privacy

- **Differential Privacy as a Mutual Information Constraint** 43
  Paul Cuff, Lanqing Yu *(Princeton University)*
- **Advanced Probabilistic Couplings for Differential Privacy** 55
  Gilles Barthe *(IMDEA Software Institute)*, Noémie Fong *(Ecole Normale Superieure)*,
  Marco Gaboardi *(University at Buffalo, SUNY)*, Benjamin Grégoire *(INRIA)*,
  Justin Hsu *(University of Pennsylvania)*, Pierre-Yves Strub *(IMDEA Software Institute)*
- **Differentially Private Bayesian Programming** 68
  Gilles Barthe *(IMDEA Software)*, Gian Pietro Farina, Marco Gaboardi *(University a Buffalo, SUNY)*,
  Emilio Jesús Gallego Arias *(CRI Mines-ParisTech)*, Andy Gordon *(Microsoft Research)*,
  Justin Hsu *(University of Pennsylvania)*, Pierre-Yves Strub *(IMDEA Software)*

Paper Session 1C: Android Security

- **The Misuse of Android Unix Domain Sockets and Security Implications** 80
  Yuru Shao *(University of Michigan)*, Jason Ott *(University of California, Riverside)*,
  Yunhan Jack Jia *(University of Michigan)*, Zhiyun Qian *(University of California, Riverside)*,
  Z. Morley Mao *(University of Michigan)*
- **Call Me Back! Attacks on System Server and System Apps in Android through Synchronous Callback** 92
  Kai Wang, Yuqing Zhang *(University of Chinese Academy of Sciences)*,
  Peng Liu *(The Pennsylvania State University)*
- **Draco: A System for Uniform and Fine-grained Access Control for Web Code on Android** 104
  Guliz Seray Tuncay, Soteris Demetriou, Carl A. Gunter *(University of Illinois at Urbana-Champaign)*

Paper Session 1D: Hardware Protection

- **Strong Non-Interference and Type-Directed Higher-Order Masking** 116
  Gilles Barthe *(IMDEA Software Institute)*, Sonia Belaïd *(Thales Communications & Security)*,
  François Dupressoir *(IMDEA Software Institute)*, Pierre-Alain Fouque *(Université de Rennes 1)*,
  Benjamin Grégoire *(Inria Sophia-Antipolis – Méditerranée)*, Pierre-Yves Strub *(IMDEA Software Institute)*,
  Rébecca Zucchini *(Inria Sophia-Antipolis – Méditerranée & École Normale Supérieure de Cachan)*

- **MERS: Statistical Test Generation for Side-Channel Analysis based Trojan Detection** 130
  Yuanwen Huang, Swarup Bhunia, Prabhat Mishra *(University of Florida)*

- **Private Circuits III: Hardware Trojan-Resilience via Testing Amplification** 142
  Stefan Dziembowski *(University of Warsaw)*, Sebastian Faust *(Ruhr-University Bochum)*,
  François-Xavier Standaert *(Universite catholique de Louvain)*

Paper Session 2A: Blockchain II

- **On the Instability of Bitcoin without the Block Reward** 154
  Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, Arvind Narayanan *(Princeton University)*

- **Transparency Overlays and Applications** 168
  Melissa Chase *(Microsoft Research)*, Sarah Meiklejohn *(University College London)*

Paper Session 2B: Differentially Private Systems I

- **EpicRec: Towards Practical Differentially Private Framework for Personalized Recommendation** 180
  Yilin Shen, Hongxia Jin *(Samsung Research America)*

- **Heavy Hitter Estimation over Set-Valued Data with Local Differential Privacy** 192
  Zhan Qin *(Hamad Bin Khalifa University & State University of New York at Buffalo)*,
  Yin Yang, Ting Yu, Issa Khalil *(Hamad Bin Khalifa University)*,
  Xiaokui Xiao *(Nanyang Technological University)*, Kui Ren *(State University of New York at Buffalo)*

Paper Session 2C: Access Control

- **AUDACIOUS: User-Driven Access Control with Unmodified Operating Systems** 204
  Talia Ringer, Dan Grossman, Franziska Roesner *(University of Washington)*

- **Mix&Slice: Efficient Access Revocation in the Cloud** 217
  Enrico Bacis *(Università di Bergamo)*,
  Sabrina De Capitani di Vimercati, Sara Foresti *(Università degli Studi di Milano)*,
  Stefano Paraboschi, Marco Rosa *(Università di Bergamo)*,
  Pierangela Samarati *(Università degli Studi di Milano)*

Paper Session 2D: Security and Persistence

- **Safe Serializable Secure Scheduling: Transactions and the Trade-Off Between Security and Consistency** 229
  Isaac Sheff, Tom Magrino, Jed Liu, Andrew C. Myers, Robbert van Renesse *(Cornell University)*

- **ProvUSB: Block-level Provenance-Based Data Protection for USB Storage Devices** 242
  Dave (Jing) Tian *(University of Florida)*, Adam Bates *(University of Illinois at Urbana-Champaign)*,
  Kevin R.B. Butler *(University of Florida)*, Raju Rangaswami *(Florida International University)*

Paper Session 3A: Smart Contracts

- **Making Smart Contracts Smarter** 254
  Loi Luu, Duc-Hiep Chu *(National University of Singapore)*,
  Hrishi Olickel *(Yale-NUS College)*,
  Prateek Saxena *(National University of Singapore)*,
  Aquinas Hobor *(Yale-NUS College & National University of Singapore)*

- **Town Crier: An Authenticated Data Feed for Smart Contracts** 270
  Fan Zhang, Ethan Cecchetti, Kyle Croman *(Cornell University)*, Ari Juels *(Cornell Tech, Jacobs Institute)*,
  Elaine Shi *(Cornell University)*

- **The Ring of Gyges: Investigating the Future of Criminal Smart Contracts** 283
  Ari Juels *(Cornell Tech, Jacobs Institute)*, Ahmed Kosba *(University of Maryland)*,
  Elaine Shi *(Cornell University)*

Paper Session 3B: Differentially Private Systems II

- **DPSense: Differentially Private Crowdsourced Spectrum Sensing** 296
  Xiaocong Jin *(Arizona State University)*, Rui Zhang *(University of Delaware)*,
  Yimin Chen, Tao Li, Yanchao Zhang *(Arizona State University)*
- **Deep Learning with Differential Privacy** 308
  Martín Abadi, Andy Chu *(Google)*, Ian Goodfellow *(Open AI)*,
  H. Brendan McMahan, Ilya Mironov, Kunal Talwar, Li Zhang *(Google)*
- **Membership Privacy in MicroRNA-based Studies** 319
  Michael Backes, Pascal Berrang, Mathias Humbert, Praveen Manoharan *(Saarland University)*

Paper Session 3C: Mobile Software Analysis

- **TaintART: A Practical Multi-level Information-Flow Tracking System for Android RunTime** 331
  Mingshen Sun *(The Chinese University of Hong Kong)*, Tao Wei *(Baidu, Inc.)*,
  John C. S. Lui *(The Chinese University of Hong Kong)*
- **Statistical Deobfuscation of Android Applications** 343
  Benjamin Bichsel, Veselin Raychev, Petar Tsankov, Martin Vechev *(ETH Zurich)*
- **Reliable Third-Party Library Detection in Android and its Security Applications** 356
  Michael Backes *(Saarland University & MPI-SWS)*, Sven Bugiel, Erik Derr *(Saarland University)*

Paper Session 3D: Kernel Memory Security

- **Prefetch Side-Channel Attacks: Bypassing SMAP and Kernel ASLR** 368
  Daniel Gruss, Clémentine Maurice *(Graz University of Technology)*, Anders Fogh *(G DATA Advanced Analytics)*,
  Moritz Lipp, Stefan Mangard *(Graz University of Technology)*
- **Breaking Kernel Address Space Layout Randomization with Intel TSX** 380
  Yeongjin Jang, Sangho Lee, Taesoo Kim *(Georgia Institute of Technology)*
- **Enforcing Least Privilege Memory Views for Multithreaded Applications** 393
  Terry Ching-Hsiang Hsu *(Purdue University)*, Kevin Hoffman *(eFolder Inc.)*,
  Patrick Eugster *(Purdue University & TU Darmstadt)*, Mathias Payer *(Purdue University)*

Paper Session 4A: Secure MPC I

- **Improvements to Secure Computation with Penalties** 406
  Ranjit Kumaresan, Vinod Vaikuntanathan, Prashant Nalini Vasudevan *(Massachusetts Institute of Technology)*
- **Amortizing Secure Computation with Penalties** 418
  Ranjit Kumaresan *(Massachusetts Institute of Technology)*, Iddo Bentov *(Cornell University)*
- **MPC-Friendly Symmetric Key Primitives** 430
  Lorenzo Grassi, Christian Rechberger *(Graz University of Technology)*,
  Dragos Rotaru, Peter Scholl, Nigel P. Smart *(University of Bristol)*

Paper Session 4B: Attacks on Ciphers

- **Message-Recovery Attacks on Feistel-Based Format Preserving Encryption** 444
  Mihir Bellare *(University of California, San Diego)*, Viet Tung Hoang *(Florida State University)*,
  Stefano Tessaro *(University of California, Santa Barbara)*
- **On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN** 456
  Karthikeyan Bhargavan, Gaëtan Leurent *(Inria)*
- **A Systematic Analysis of the Juniper Dual EC Incident** 468
  Stephen Checkoway *(University of Illinois at Chicago)*, Jacob Maskiewicz *(University of California, San Diego)*,
  Christina Garman *(Johns Hopkins University)*, Joshua Fried, Shaanan Cohney *(University of Pennsylvania)*,
  Matthew Green *(Johns Hopkins University)*, Nadia Heninger *(University of Pennsylvania)*,
  Ralf-Philipp Weinmann *(Comsecuris)*, Eric Rescorla, Hovav Shacham *(University of California, San Diego)*

Paper Session 4C: Big Data Meets Security

- **Scalable Graph-based Bug Search for Firmware Images** 480
  Qian Feng, Rundong Zhou, Chengcheng Xu, Yao Cheng *(Syracuse University)*,
  Brian Testa *(Syracuse University & Air Force Research Lab)*,
  Heng Yin *(Syracuse University & University of California, Riverside)*
- **SmartWalk: Enhancing Social Network Security via Adaptive Random Walks** 492
  Yushan Liu *(Princeton University)*, Shouling Ji *(Zhejiang University & Georgia Tech)*,
  Prateek Mittal *(Princeton University)*
- **High Fidelity Data Reduction for Big Data Security Dependency Analyses** 504
  Zhang Xu *(NofutzNetworks Inc.)*,
  Zhenyu Wu, Zhichun Li, Kangkook Jee, Junghwan Rhee, Xusheng Xiao *(NEC Laboratories America Inc.)*,
  Fengyuan Xu *(Nanjing University)*, Haining Wang *(University of Delaware)*,
  Guofei Jiang *(NEC Laboratories America Inc.)*

Paper Session 4D: Types and Memory Safety

- **TypeSan: Practical Type Confusion Detection** 517
  Istvan Haller *(Vrije Universiteit Amsterdam)*, Yuseok Jeon, Hui Peng, Mathias Payer *(Purdue University)*,
  Cristiano Giuffrida, Herbert Bos, Erik van der Kouwe *(Vrije Universiteit Amsterdam)*
- **CREDAL: Towards Locating a Memory Corruption Vulnerability with Your Core Dump** 529
  Jun Xu *(The Pennsylvania State University)*,
  Dongliang Mu *(Nanjing University & The Pennsylvania State University)*,
  Ping Chen, Xinyu Xing, Pei Wang, Peng Liu *(The Pennsylvania State University)*
- **Twice the Bits, Twice the Trouble: Vulnerabilities Induced by Migrating to 64-Bit Platforms** 541
  Christian Wressnegger, Fabian Yamaguchi, Alwin Maier, Konrad Rieck *(TU Braunschweig)*

Paper Session 5A: Secure MPC II

- **Alternative Implementations of Secure Real Numbers** 553
  Vassil Dimitrov *(University of Calgary)*, Liisi Kerik *(Cybernetica)*, Toomas Krips *(STACC)*,
  Jaak Randmets *(Cybernetica)*, Jan Willemson *(Cybernetica & STACC)*
- **Garbling Gadgets for Boolean and Arithmetic Circuits** 565
  Marshall Ball, Tal Malkin *(Columbia University)*, Mike Rosulek *(Oregon State University)*
- **Optimizing Semi-Honest Secure Multiparty Computation for the Internet** 578
  Aner Ben-Efraim *(Ben-Gurion University)*, Yehuda Lindell *(Bar-Ilan University)*, Eran Omri *(Ariel University)*

Paper Session 5B: Physically Based Authentication

- **MEMS Gyroscopes as Physical Unclonable Functions** 591
  Oliver Willers, Christopher Huth *(Robert Bosch GmbH)*, Jorge Guajardo *(Robert Bosch LLC)*,
  Helmut Seidel *(Saarland University)*
- **On the Security and Usability of Segment-based Visual Cryptographic Authentication Protocols** 603
  Tianhao Wang, Huangyi Ge, Omar Chowdhury, Hemanta K. Maji, Ninghui Li *(Purdue University)*
- **Instant and Robust Authentication and Key Agreement among Mobile Devices** 616
  Wei Xi *(Xi'an Jiaotong University)*, Chen Qian *(University of California Santa Cruz)*,
  Jinsong Han, Kun Zhao *(Xi'an Jiaotong University)*, Sheng Zhong *(Nanjing University)*,
  Xiang-Yang Li *(University of Science and Technology of China)*, Jizhong Zhao *(Xi'an Jiaotong University)*

Paper Session 5C: Web Security

- **Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem** 628
  Frank Cangialosi *(University of Maryland)*, Taejoong Chung, David Choffnes *(Northeastern University)*,
  Dave Levin *(University of Maryland)*, Bruce M. Maggs *(Duke University & Akamai Technologies)*,
  Alan Mislove, Christo Wilson *(Northeastern University)*

- **Chainsaw: Chained Automated Workflow-based Exploit Generation** 641
  Abeer Alhuzali, Birhanu Eshete, Rigel Gjomemo, V.N. Venkatakrishnan *(University of Illinois at Chicago)*
- **CSPAutoGen: Black-box Enforcement of Content Security Policy upon Real-world Websites** 653
  Xiang Pan *(Northwestern University)*, Yinzhi Cao *(Lehigh University)*,
  Shuangping Liu, Yu Zhou *(Northwestern University)*,
  Yan Chen *(Zhejiang University & Northwestern University)*, Tingzhe Zhou *(Lehigh University)*

Paper Session 5D: Security Bug Finding

- **How I Learned to be Secure: A Census-Representative Survey of Security Advice Sources and Behavior** 666
  Elissa M. Redmiles *(University of Maryland)*, Sean Kross *(Johns Hopkins University)*,
  Michelle L. Mazurek *(University of Maryland)*
- **Practical Detection of Entropy Loss in Pseudo-Random Number Generators** 678
  Felix Dörre, Vladimir Klebanov *(Karlsruhe Institute of Technology)*
- **Build It, Break It, Fix It: Contesting Secure Development** 690
  Andrew Ruef, Michael Hicks, James Parker, Dave Levin, Michelle L. Mazurek *(University of Maryland)*,
  Piotr Mardziel *(Carnegie Mellon University)*

Paper Session 6A: Phone Security using Formal Methods

- **SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles** 704
  Luke Deshotels *(North Carolina State University)*,
  Razvan Deaconescu, Mihai Chiroiu *(University Politehnica of Bucharest)*,
  Lucas Davi *(Technische Universitat Darmstadt)*, William Enck *(North Carolina State University)*,
  Ahmad-Reza Sadeghi *(Technische Universitat Darmstadt)*
- **Computational Soundness for Dalvik Bytecode** 717
  Michael Backes, Robert Künnemann *(Saarland University & MPI-SWS)*, Esfandiar Mohammadi *(ETH Zurich)*

Paper Session 6B: Attestation

- **SANA: Secure and Scalable Aggregate Network Attestation** 731
  Moreno Ambrosin, Mauro Conti *(University of Padua)*, Ahmad Ibrahim *(Technische Universität Darmstadt)*,
  Gregory Neven *(IBM Research - Zurich)*, Ahmad-Reza Sadeghi *(Technische Universität Darmstadt)*,
  Matthias Schunter *(Intel Labs - Darmstadt)*
- **C-FLAT: Control-Flow Attestation for Embedded Systems Software** 743
  Tigist Abera *(Technische Universität Darmstadt)*, N. Asokan *(Aalto University)*,
  Lucas Davi *(Technische Universität Darmstadt)*, Jan-Erik Ekberg *(Trustonic)*,
  Thomas Nyman *(Aalto University & Trustonic)*, Andrew Paverd *(Aalto University)*,
  Ahmad-Reza Sadeghi *(Technische Universität Darmstadt)*, Gene Tsudik *(University of California, Irvine)*

Paper Session 6C: Mine your Literature

- **Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence** 755
  Xiaojing Liao *(Georgia Institute of Technology)*, Kan Yuan, XiaoFeng Wang *(Indiana University Bloomington)*,
  Zhou Li *(ACM Member)*, Luyi Xing *(Indiana University Bloomington)*,
  Raheem Beyah *(Georgia Institute of Technology)*
- **FeatureSmith: Automatically Engineering Features for Malware Detection by Mining the Security Literature** 767
  Ziyun Zhu, Tudor Dumitras *(University of Maryland, College Park)*

Paper Session 6D: Security Studies

- **An In-Depth Study of More Than Ten Years of Java Exploitation** 779
  Philipp Holzinger, Stefan Triller *(Fraunhofer SIT)*, Alexandre Bartel *(Technische Universität Darmstadt)*,
  Eric Bodden *(Paderborn University & Fraunhofer IEM)*
- **"The Web/Local" Boundary Is Fuzzy: A Security Study of Chrome's Process-based Sandboxing** 791
  Yaoqi Jia, Zheng Leong Chua, Hong Hu *(National University of Singapore)*, Shuo Chen *(Microsoft Research)*,
  Prateek Saxena, Zhenkai Liang *(National University of Singapore)*

Paper Session 7A: Secure MPC III

- **High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority** 805
  Toshinori Araki, Jun Furukawa *(NEC Corporation)*, Yehuda Lindell, Ariel Nof *(Bar-Ilan University)*,
  Kazuma Ohara *(NEC Corporation)*
- **Efficient Batched Oblivious PRF with Applications to Private Set Intersection** 818
  Vladimir Kolesnikov *(Bell Labs)*, Ranjit Kumaresan *(Massachusetts Institute of Technology)*,
  Mike Rosulek, Ni Trieu *(Oregon State University)*
- **MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer** 830
  Marcel Keller, Emmanuela Orsini, Peter Scholl *(University of Bristol)*

Paper Session 7B: Side-Channel Attacks

- **Covert Channels through Random Number Generator: Mechanisms, Capacity Estimation and Mitigations** 843
  Dmitry Evtyushkin, Dmitry Ponomarev *(SUNY Binghamton)*
- **Return-Oriented Flush-Reload Side Channels on ARM and Their Implications for Android Devices** 858
  Xiaokuan Zhang, Yuan Xiao, Yinqian Zhang *(The Ohio State University)*
- **A Software Approach to Defeating Side Channels in Last-Level Caches** 871
  Ziqiao Zhou, Michael K. Reiter *(University of North Carolina)*, Yinqian Zhang *(The Ohio State University)*

Paper Session 7C: Acoustic Attacks

- **Leave Your Phone at the Door:Side Channels that Reveal Factory Floor Secrets** 883
  Avesta Hojjati *(University of Illinois at Urbana-Champaign)*,
  Anku Adhikari *(University of Illinois at Urbana-Champaign & Advanced Digital Sciences Center)*,
  Katarina Struckmann, Edward Chou *(University of Illinois at Urbana-Champaign)*,
  Thi Ngoc Tho Nguyen *(Advanced Digital Sciences Center)*,
  Kushagra Madan *(University of Illinois at Urbana-Champaign)*,
  Marianne S. Winslett *(University of Illinois at Urbana-Champaign & Advanced Digital Sciences Center)*,
  Carl A. Gunter, William P. King *(University of Illinois at Urbana-Champaign)*
- **My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks Against 3D Printers** 895
  Chen Song, Feng Lin, Zhongjie Ba, Kui Ren, Chi Zhou, Wenyao Xu *(University at Buffalo, SUNY)*
- **The Sounds of the Phones: Dangers of Zero-Effort Second Factor Login based on Ambient Audio** 908
  Babins Shrestha, Maliheh Shirvanian, Prakash Shrestha, Nitesh Saxena *(University of Alabama at Birmingham)*

Paper Session 7D: Protection Across Executions

- **UniSan: Proactive Kernel Memory Initialization to Eliminate Data Leakages** 920
  Kangjie Lu, Chengyu Song, Taesoo Kim, Wenke Lee *(Georgia Institute of Technology)*
- **iLock: Immediate and Automatic Locking of Mobile Devices against Data Theft** 933
  Tao Li, Yimin Chen, Jingchao Sun, Xiaocong Jin, Yanchao Zhang *(Arizona State University)*
- **Hypnoguard: Protecting Secrets across Sleep-wake Cycles** 945
  Lianying Zhao, Mohammad Mannan *(Concordia University)*

Paper Session 8A: Lattices and Obfuscation

- **5Gen: A Framework for Prototyping Applications Using Multilinear Maps and Matrix Branching Programs** 981
  Kevin Lewi *(Stanford University)*, Alex J. Malozemoff *(Galois)*, Daniel Apon *(University of Maryland)*, Brent Carmer *(Oregon State University)*, Adam Foltzer, Daniel Wagner, David W. Archer *(Galois)*, Dan Boneh *(Stanford University)*, Jonathan Katz *(University of Maryland)*, Mariana Raykova *(Yale University)*
- **Λολ: Functional Lattice Cryptography** 993
  Eric Crockett, Chris Peikert *(University of Michigan)*
- **Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE** 1006
  Joppe Bos *(NXP Semiconductors)*, Craig Costello *(Microsoft Research)*, Leo Ducas *(CWI)*, Ilya Mironov *(Google, Inc.)*, Michael Naehrig *(Microsoft Research)*, Valeria Nikolaenko *(Stanford University)*, Ananth Raghunathan *(Google, Inc.)*, Douglas Stebila *(McMaster University)*

Paper Session 8B: Attacks and Defenses

- **On Code Execution Tracking via Power Side-Channel** 1019
  Yannan Liu, Lingxiao Wei, Zhe Zhou, Kehuan Zhang *(The Chinese University of Hong Kong)*, Wenyuan Xu *(Zhejiang University)*, Qiang Xu *(The Chinese University of Hong Kong)*
- **Coverage-based Greybox Fuzzing as Markov Chain** 1032
  Marcel Böhme, Van-Thuan Pham, Abhik Roychoudhury *(National University of Singapore)*
- **Error Handling of In-vehicle Networks Makes Them Vulnerable** 1044
  Kyong-Tak Cho, Kang G. Shin *(The University of Michigan)*

Paper Session 8C: Phone Security

- **Using Reflexive Eye Movements for Fast Challenge-Response Authentication** 1056
  Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen , Ivan Martinovic *(University of Oxford)*
- **When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals** 1068
  Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu *(Shanghai Jiao Tong University)*, Xiaohui Liang *(University of Massachusetts at Boston)*, Yao Liu *(University of South Florida)*, Na Ruan *(Shanghai Jiao Tong University)*
- **VoiceLive: A Phoneme Localization based Liveness Detection for Voice Authentication on Smartphones** 1080
  Linghan Zhang, Sheng Tan, Jie Yang *(Florida State University)*, Yingying Chen *(Stevens Institute of Technology)*

Paper Session 8D: Infrastructure Attacks

- **Limiting the Impact of Stealthy Attacks on Industrial Control Systems** 1092
  David I. Urbina, Jairo Giraldo, Alvaro A. Cardenas *(University of Texas at Dallas)*, Nils Ole Tippenhauer *(Singapore University of Technology and Design)*, Junia Valente, Mustafa Faisal, Justin Ruths *(University of Texas at Dallas)*, Richard Candell *(National Institute of Standards and Technology)*, Henrik Sandberg *(KTH Royal Institute of Technology)*
- **Over-The-Top Bypass: Study of a Recent Telephony Fraud** 1106
  Merve Sahin *(Eurecom & Monaco Digital Security Agency)*, Aurélien Francillon *(Eurecom)*
- **New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks** 1118
  Guan-Hua Tu *(Michigan State University)*, Chi-Yu Li *(National Chiao Tung University)*, Chunyi Peng *(Ohio State University)*, Yuanjie Li, Songwu Lu *(University of California, Los Angeles)*

Paper Session 9A: Order-Revealing and Searchable Encryption

- **POPE: Partial Order Preserving Encoding** 1131
  Daniel S. Roche *(United States Naval Academy)*, Daniel Apon *(University of Maryland)*, Seung Geol Choi *(United States Naval Academy)*, Arkady Yerukhimovich *(MIT Lincoln Laboratory)*
- **Σοφος – Forward Secure Searchable Encryption** 1143
  Raphael Bost *(Université de Rennes 1)*

- **What Else is Revealed by Order-Revealing Encryption?** 1155
  F. Betül Durak *(Rutgers University)*, Thomas M. DuBuisson *(Galois, Inc.)*, David Cash *(Rutgers University)*
- **Order-Revealing Encryption: New Constructions, Applications, and Lower Bounds** 1167
  Kevin Lewi, David J. Wu *(Stanford University)*

Paper Session 9B: Authentication

- **Practical Anonymous Password Authentication and TLS with Anonymous Client Authentication** 1179
  Zhenfeng Zhang, Kang Yang, Xuexian Hu, Yuchen Wang *(Chinese Academy of Sciences)*
- **Efficient Cryptographic Password Hardening Services from Partially Oblivious Commitments** 1192
  Jonas Schneider, Nils Fleischhacker *(Saarland University)*,
  Dominique Schröder *(Friedrich-Alexander-University)*, Michael Backes *(Saarland University)*
- **A Comprehensive Formal Security Analysis of OAuth 2.0** 1204
  Daniel Fett, Ralf Küsters, Guido Schmitz *(University of Trier)*

Paper Session 9C: Passwords

- **An Empirical Study of Mnemonic Sentence-based Password Generation Strategies** 1216
  Weining Yang, Ninghui Li, Omar Chowdhury, Aiping Xiong, Robert W. Proctor *(Purdue University)*
- **On the Security of Cracking-Resistant Password Vaults** 1230
  Maximilian Golla, Benedict Beuscher, Markus Dürmuth *(Ruhr-University Bochum)*
- **Targeted Online Password Guessing: An Underestimated Threat** 1242
  Ding Wang, Zijian Zhang, Ping Wang *(Peking University)*, Jeff Yan *(Lancaster University)*,
  Xinyi Huang *(Fujian Normal University)*

Paper Session 9D: Internet Security

- **PIPSEA: A Practical IPsec Gateway on Embedded APUs** 1255
  Jungho Park *(Seoul National University & ManyCoreSoft Co., Ltd.)*, Wooken Jung *(Seoul National University)*,
  Gangwon Jo *(Seoul National University & ManyCoreSoft Co., Ltd.)*,
  Ilkoo Lee, Jaejin Lee *(Seoul National University)*
- **MiddlePolice: Toward Enforcing Destination-Defined Policies in the Middle of the Internet** 1268
  Zhuotao Liu *(University of Illinois at Urbana-Champaign)*, Hao Jin *(Nanjing University)*,
  Yih-Chun Hu, Michael Bailey *(University of Illinois at Urbana-Champaign)*
- **Protecting Insecure Communications with Topology-aware Network Tunnels** 1280
  Georgios Kontaxis, Angelos D. Keromytis *(Columbia University)*

Paper Session 10A: Specialized Crypto Tools

- **Function Secret Sharing: Improvements and Extensions** 1292
  Elette Boyle *(IDC Herzliya)*, Niv Gilboa *(Ben Gurion University)*,
  Yuval Ishai *(Technion and University of California, Los Angeles)*
- **Hash First, Argue Later: Adaptive Verifiable Computations on Outsourced Data** 1304
  Dario Fiore *(IMDEA Software Institute)*, Cédric Fournet *(Microsoft Research)*, Esha Ghosh *(Brown University)*,
  Markulf Kohlweiss, Olga Ohrimenko, Bryan Parno *(Microsoft Research)*
- **Practical Non-Malleable Codes from l-more Extractable Hash Functions** 1317
  Aggelos Kiayias *(University of Edinburgh)*, Feng-Hao Liu *(Florida Atlantic University)*,
  Yiannis Tselekounis *(University of Edinburgh)*

Paper Session 10B: Crypto Implementations -- used to be 11B

- **A Surfeit of SSH Cipher Suites** 1480
  Martin R. Albrecht, Jean Paul Degabriele, Torben Brandt Hansen, Kenneth G. Paterson
  (Royal Holloway, University of London)
- **Systematic Fuzzing and Testing of TLS Libraries** 1492
  Juraj Somorovsky *(Ruhr University Bochum)*
- **Attacking OpenSSL Implementation of ECDSA with a Few Signatures** 1505
  Shuqin Fan *(State Key Laboratory of Cryptology)*, Wenbo Wang *(Luoyang University of Foreign Languages)*,
  Qingfeng Cheng *(Xidian University)*

Paper Session 10C: Measuring Security in the Wild

- **Content Security Problems? Evaluating the Effectiveness of Content Security Policy in the Wild** 1365
  Stefano Calzavara, Alvise Rabitti, Michele Bugliesi *(Università Ca' Foscari)*
- **CSP Is Dead, Long Live CSP! On the Insecurity of Whitelists and the Future of Content Security Policy** 1376
  Lukas Weichselbaum, Michele Spagnuolo, Sebastian Lekies, Artur Janc *(Google, Inc.)*
- **Online Tracking: A 1-million-site Measurement and Analysis** 1388
  Steven Englehardt, Arvind Narayanan *(Princeton University)*

Paper Session 10D: Network Security I

- **PhishEye: Live Monitoring of Sandboxed Phishing Kits** 1402
  Xiao Han *(Orange Labs & Eurecom)*, Nizar Kheir *(Orange Labs)*, Davide Balzarotti *(Eurecom)*
- **All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records** 1414
  Daiping Liu *(University of Delaware)*, Shuai Hao *(College of William and Mary)*,
  Haining Wang *(University of Delaware)*
- **Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks** 1426
  Johannes Krupp *(Saarland University)*, Michael Backes *(Saarland University & MPI-SWS)*,
  Christian Rossow *(Saarland University)*

Paper Session 11A: Key Exchange

- **A Unilateral-to-Mutual Authentication Compiler for Key Exchange (with Applications to Client Authentication in TLS 1.3)** 1438
  Hugo Krawczyk *(IBM Research)*
- **Attribute-based Key Exchange with General Policies** 1451
  Vladimir Kolesnikov *(Bell Labs)*, Hugo Krawczyk *(IBM Research)*, Yehuda Lindell *(Bar-Ilan University)*,
  Alex Malozemoff *(Galois)*, Tal Rabin *(IBM Research)*
- **Identity-Concealed Authenticated Encryption and Key Exchange** 1464
  Yunlei Zhao *(Fudan University)*

Paper Session 11B: Attacks using a Little Leakage – used to be 10B

- **Generic Attacks on Secure Outsourced Databases** 1329
  Georgios Kellaris *(Boston University & Harvard University)*, George Kollios *(Boston University)*,
  Kobbi Nissim *(Ben-Gurion University & Harvard University)*, Adam O'Neill *(Georgetown University)*
- **The Shadow Nemesis: Inference Attacks on Efficiently Deployable, Efficiently Searchable Encryption** 1341
  David Pouliot, Charles V. Wright *(Portland State University)*
- **Breaking Web Applications Built On Top of Encrypted Data** 1353
  Paul Grubbs *(Cornell University)*, Richard McPherson *(University of Texas at Austin)*,
  Muhammad Naveed *(University of Southern California)*,
  Thomas Ristenpart, Vitaly Shmatikov *(Cornell Tech)*

Paper Session 11C: More Attacks

- **Host of Troubles: Multiple Host Ambiguities in HTTP Implementations** 1516
Jianjun Chen *(Tsinghua University & Tsingua National Laboratory for Information Science and Technology)*,
Jian Jiang *(University of California, Berkeley)*,
Haixin Duan *(Tsinghua University & Tsingua National Laboratory for Information Science and Technology)*,
Nicholas Weaver *(University of California, Berkeley & ICSI)*,
Tao Wan *(Huawei Canada)*,
Vern Paxson *(University of California, Berkeley & ICSI)*

- **Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition** 1528
Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer *(Carnegie Mellon University)*,
Michael K. Reiter *(University of North Carolina)*

- **Lurking Malice in the Cloud: Understanding and Detecting Cloud Repository as a Malicious Service** 1541
Xiaojing Liao *(Georgia Institute of Technology)*,
Sumayah Alrwais, Kan Yuan, Luyi Xing, XiaoFeng Wang *(Indiana University Bloomington)*,
Shuang Hao *(University of California Santa Barbara)*,
Raheem Beyah *(Georgia Institute of Technology)*

Paper Session 11D: Network Security II

- **Safely Measuring Tor** 1553
Rob Jansen, Aaron Johnson *(US Naval Research Laboratory)*

- **PREDATOR: Proactive Recognition and Elimination of Domain Abuse at Time-of-Registration** 1568
Shuang Hao, Alex Kantchelian *(University of California, Berkeley)*, Brad Miller *(Google, Inc.)*,
Vern Paxson *(University of California, Berkeley & International Computer Science Institute)*,
Nick Feamster *(Princeton University)*

- **Stemming Downlink Leakage from Training Sequences in Multi-User MIMO Networks** 1580
Yunlong Mao, Yuan Zhang, Sheng Zhong *(Nanjing University)*

Paper Session 12A: Secure Protocols

- **A Protocol for Privately Reporting Ad Impressions at Scale** 1591
Matthew Green *(Johns Hopkins University)*, Watson Ladd *(University of California, Berkeley)*,
Ian Miers *(Johns Hopkins University)*

- **Secure Stable Matching at Scale** 1602
Jack Doerner, David Evans *(University of Virginia)*, abhi shelat *(Northeastern University)*

- **BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme** 1614
Pyrros Chaidos *(University College London)*,
Véronique Cortier *(LORIA, CNRS & INRIA & Université de Lorraine)*,
Georg Fuchsbauer *(Inria, ENS, CNRS, PSL Research University)*, David Galindo *(University of Birmingham)*

Paper Session 12B: DSA/ECDSA

- **ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels** 1626
Daniel Genkin *(Technion and Tel Aviv University)*,
Lev Pachmanov, Itamar Pipman, Eran Tromer *(Tel Aviv University)*,
Yuval Yarom *(The University of Adelaide & Data61, CSIRO)*

- **"Make Sure DSA Signing Exponentiations Really are Constant-Time"** 1639
Cesar Pereida García *(Aalto University)*, Billy Bob Brumley *(Tampere University of Technology)*,
Yuval Yarom *(The University of Adelaide & Data61)*

- **On the Provable Security of (EC)DSA Signatures** 1651
Manuel Fersch, Eike Kiltz, Bertram Poettering *(Ruhr University Bochum)*

Paper Session 12C: Even more Attacks

- **Android ION Hazard: The Curse of Customizable Memory Management System** 1663
Hang Zhang, Dongdong She, Zhiyun Qian *(University of California, Riverside)*
- **Drammer: Deterministic Rowhammer Attacks on Mobile Platforms** 1675
Victor van der Veen *(Vrije Universiteit Amsterdam)*,
Yanick Fratantonio, Martina Lindorfer *(University of California, Santa Barbara)*,
Daniel Gruss, Clémentine Maurice *(Graz University of Technology)*,
Giovanni Vigna *(University of California, Santa Barbara)*,
Herbert Bos, Kaveh Razavi, Cristiano Giuffrida *(Vrije Universiteit Amsterdam)*
- **SFADiff: Automated Evasion Attacks and Fingerprinting Using Black-box Differential Automata Learning** 1690
George Argyros *(Columbia University)*, Ioannis Stais *(University of Athens)*,
Suman Jana, Angelos D. Keromytis *(Columbia University)*, Aggelos Kiayias *(University of Edinburgh)*

Paper Session 12D: Anonymous Communication

- **Slitheen: Perfectly Imitated Decoy Routing through Traffic Replacement** 1702
Cecylia Bocovich, Ian Goldberg *(University of Waterloo)*
- **Practical Censorship Evasion Leveraging Content Delivery Networks** 1715
Hadi Zolfaghari, Amir Houmansadr *(University of Massachusetts, Amherst)*
- **GAME OF DECOYS: Optimal Decoy Routing Through Game Theory** 1727
Milad Nasr, Amir Houmansadr *(University of Massachusetts, Amherst)*

Posters

- **POSTER: An Educational Network Protocol for Covert Channel Analysis Using Patterns** 1739
Steffen Wendzel *(Worms University of Applied Sciences)*,
Wojciech Mazurczyk *(Warsaw University of Technology)*
- **POSTER: A Behavioural Authentication System for Mobile Users** 1742
Md Morshedul Islam, Reihaneh Safavi-Naini *(University of Calgary)*
- **POSTER: A Keyless Efficient Algorithm for Data Protection by Means of Fragmentation** 1745
Katarzyna Kapusta, Gerard Memmi, Hassan Noura *(Telecom ParisTech Universite Paris-Saclay)*
- **POSTER: Accuracy vs. Time Cost: Detecting Android Malware through Pareto Ensemble Pruning** 1748
Lingling Fan *(East China Normal University)*, Minhui Xue *(East China Normal University & NYU Shanghai)*,
Sen Chen, Lihua Xu *(East China Normal University)*, Haojin Zhu *(Shanghai Jiao Tong University)*
- **POSTER: Attack on Non-Linear Physical Unclonable Function** 1751
Jing Ye, Yu Hu, Xiaowei Li *(Chinese Academy of Sciences)*
- **POSTER: ConcurORAM: High-Throughput Parallel Multi-Client ORAM** 1754
Anrin Chakraborti, Radu Sion *(Stony Brook University)*
- **POSTER: DataLair - A Storage Block Device with Plausible Deniability** 1757
Anrin Chakraborti, Chen Chen, Radu Sion *(Stony Brook University)*
- **POSTER: DroidShield: Protecting User Applications from Normal World Access** 1760
Darius Suciu, Radu Sion *(Stony Brook University)*
- **POSTER: Efficient Cross-User Chunk-Level Client-Side Data Deduplication with Symmetrically Encrypted Two-Party Interactions** 1763
Chia-Mu Yu *(National Chung Hsing University)*
- **POSTER: Fingerprinting Tor Hidden Services** 1766
Asya Mitseva, Andriy Panchenko *(University of Luxembourg)*, Fabian Lanze *(Huf Secure Mobile GmbH)*,
Martin Henze, Klaus Wehrle *(RWTH Aachen University)*, Thomas Engel *(University of Luxembourg)*

- **POSTER: I Don't Want That Content! On the Risks of Exploiting Bitcoin's Blockchain as a Content Store** 1769
  Roman Matzutt, Oliver Hohlfeld, Martin Henze, Robin Rawiel, Jan Henrik Ziegeldorf, Klaus Wehrle
  (RWTH Aachen University)
- **POSTER: Identifying Dynamic Data Structures in Malware** 1772
  Thomas Rupprecht *(University of Bamberg)*, Xi Chen *(Vrije Universiteit Amsterdam)*,
  David H. White *(University of Bamberg)*, Jan Tobias Mühlberg *(KU Leuven)*,
  Herbert Bos *(Vrije Universiteit Amsterdam)*, Gerald Lüttgen *(University of Bamberg)*
- **POSTER: Improved Markov Strength Meters for Passwords** 1775
  Harshal Tupsamudre, Vijayanand Banahatti, Sachin Lodha *(TCS Research)*
- **POSTER: Insights of Antivirus Relationships when Detecting Android Malware: A Data Analytics Approach** 1778
  Ignacio Martín, José Alberto Hernández *(Universidad Carlos II)*,
  Sergio de los Santos, Antonio Guzmán *(Telefónica Digital Identity & Privacy)*
- **POSTER: KXRay: Introspecting the Kernel for Rootkit Timing Footprints** 1781
  Chen Chen, Darius Suciu, Radu Sion *(Stony Brook University)*
- **POSTER: Locally Virtualized Environment for Mitigating Ransomware Threat** 1784
  Manish Shukla, Sutapa Mondal, Sachin Lodha *(TCS Research)*
- **POSTER: Mapping the Landscape of Large-Scale Vulnerability Notifications** 1787
  Ben Stock, Giancarlo Pellegrino, Christian Rossow *(Saarland University)*, Martin Johns *(SAP SE)*,
  Michael Backes *(Saarland University & MPI-SWS)*
- **POSTER: Phishing Website Detection with a Multiphase Framework to Find Visual Similarity** 1790
  Omid Asudeh *(University of Texas at Arlington)*, Mathew Wright *(Rochester Institute of Technology)*
- **POSTER: Privacy Enhanced Secure Location Verification** 1793
  Md Mamunur Rashid Akand, Reihaneh Safavi-Naini *(University of Calgary)*
- **POSTER: Re-Thinking Risks and Rewards for Trusted Third Parties** 1796
  Jan-Ole Malchow, Benjamin Güldenring, Volker Roth *(Freie Universität Berlin)*
- **POSTER: RIA – An Audition-based Method to Protect the Runtime Integrity of MapReduce Applications** 1799
  Yongzhi Wang, Yulong Shen *(Xidian University)*
- **POSTER: Security Enhanced Administrative Role Based Access Control Models** 1802
  Rajkumar P.V. *(Texas Southern University)*, Ravi Sandhu *(University of Texas San Antonio)*
- **POSTER: (Semi)-Supervised Machine Learning Approaches for Network Security in High-Dimensional Network Data** 1805
  Pedro Casas, Alessandro D'Alconzo, Giuseppe Settanni *(AIT Austrian Institute of Technology)*,
  Pierdomenico Fiadino *(Eurecat Technology Centre of Catalonia)*,
  Florian Skopik *(AIT Austrian Institute of Technology)*
- **POSTER: Static ROP Chain Detection Based on Hidden Markov Model Considering ROP Chain Integrity** 1808
  Toshinori Usui *(NTT Secure Platform Laboratories)*, Tomonori Ikuse *(NTT Security (Japan) KK)*,
  Makoto Iwamura, Takeshi Yada *(NTT Secure Platform Laboratories)*
- **POSTER: The ART of App Compartmentalization** 1811
  Michael Backes *(Saarland University & MPI-SWS)*,
  Sven Bugiel, Jie Huang, Oliver Schranz *(Saarland University)*
- **Poster: Toward Automating the Generation of Malware Analysis Reports Using the Sandbox Logs** 1814
  Bo Sun, Akinori Fujino, Tatsuya Mori *(Waseda University)*
- **POSTER: Towards Collaboratively Supporting Decision Makers in Choosing Suitable Authentication Schemes** 1817
  Peter Mayer, Stephan Neumann, Melanie Volkamer *(Technische Universität Darmstadt)*
- **POSTER: Towards Exposing Internet of Things: A Roadmap** 1820
  Vinay Sachidananda, Jinghui Toh *(Singapore University of Technology and Design)*,
  Shachar Siboni, Asaf Shabtai *(Ben-Gurion University of the Negev)*,
  Yuval Elovici *(Singapore University of Technology and Design)*

- **POSTER: Towards Highly Interactive Honeypots for Industrial Control Systems** 1823
Stephan Lau, Johannes Klick, Stephan Arndt, Volker Roth *(Freie Universität Berlin)*
- **POSTER: Towards Privacy-Preserving Biometric Identification in Cloud Computing** 1826
Changhee Hahn, Junbeom Hur *(Korea University)*
- **POSTER: VUDEC – A Framework for Vulnerability Management in Decentralized Communication Networks** 1829
Michael Steinke *(Universität der Bundeswehr München)*, Stefan Metzger *(Leibniz Supercomputing Center)*, Wolfgang Hommel *(Universität der Bundeswehr München)*
- **POSTER: Weighing in eHealth Security: A Security and Privacy Study of Smart Scales** 1832
Martin Krämer, David Aspinall, Maria Wolters *(University of Edinburgh)*
- **POSTER: WiPING: Wi-Fi signal-based PIN Guessing attack** 1835
Seunghun Cha, Jaewoo Park, Geumhwan Cho *(Sungkyunkwan University)*, Jun Ho Huh *(Honeywell ACS Labs)*, Hyoungshick Kim *(Sungkyunkwan University)*

Demonstrations

- **DEMO: Easy Deployment of a Secure Internet Architecture for the 21st Century: How Hard Can It Be to Build a Secure Internet?** 1838
Ercan Ucan, Raphael M. Reischuk, Adrian Perrig *(ETH Zurich)*
- **Demo: High-Throughput Secure Three-Party Computation of Kerberos Ticket Generation** 1841
Toshinori Araki *(NEC Corporation)*, Assaf Barak *(Bar-Ilan University)*, Jun Furukawa *(NEC Corporation)*, Yehuda Lindell, Ariel Nof *(Bar-Ilan University)*, Kazuma Ohara *(NEC Corporation)*
- **DEMO: Integrating MPC in Big Data Workflows** 1844
Nikolaj Volgushev *(Boston University)*, Malte Schwarzkopf *(Massachusetts Institute of Technology)*, Andrei Lapets, Mayank Varia, Azer Bestavros *(Boston University)*
- **DEMO: OffPAD – Offline Personal Authenticating Device with Applications in Hospitals and e-Banking** 1847
Denis Migdal *(Ecole Nationale Supérieure d'Ingénieurs de Caen)*, Christian Johansen, Audun Jøsang *(University of Oslo)*
- **DEMO: Starving Permission-Hungry Android Apps Using SecuRank** 1850
Vincent F. Taylor, Ivan Martinovic *(University of Oxford)*

Tutorials

- **Program Anomaly Detection: Methodology and Practices** 1853
Xiaokui Shu *(IBM Research)*, Danfeng Yao *(Virginia Tech)*
- **Security on Wheels: Security and Privacy for Vehicular Communication Systems** 1855
Panos Papadimitratos *(KTH Royal Institute of Technology)*
- **Condensed Cryptographic Currencies Crash Course (C5)** 1857
Aljosha Judmayer *(SBA Research)*, Edgar Weippl *(SBA Research)*
- **Introduction to Credit Networks: Security, Privacy, and Applications** 1859
Aniket Kate *(Purdue University)*
- **On the Security and Scalability of Bitcoin's Blockchain** 1861
Ghassan Karame *(NEC Laboratories Europe)*
- **Privacy and Security in the Genomic Era** 1863
Erman Ayday *(Bilkent University)*, Jean-Pierre Hubaux *(École Polytechnique Fédérale de Lausanne)*
- **Adversarial Data Mining: Big Data Meets Cyber Security** 1866
Murat Kantarcioglu *(University of Texas at Dallas)*, Bowei Xi *(Purdue University)*

Pre-Conference Workshops co-located with CCS 2016

- **MTD 2016: Third ACM Workshop on Moving Target Defense** 1868
  Peng Liu *(Penn State University)*, Cliff Wang *(U.S. Army Research Office)*
- **PLAS'16 – ACM SIGPLAN 11th Workshop on Programming Languages and Analysis for Security** 1870
  Toby Murray *(University of Melbourne & Data61)*,
  Deian Stefan *(University of California, San Diego & Intrinsic)*
- **SafeConfig'16 – Testing and Evaluation for Active and Resilient Cyber Systems** 1871
  Nicholas J. Multari *(Pacific Northwest National Lab)*,
  Anoop Singhal *(National Institute of Standards and Technology)*,
  David O. Manz *(Pacific Northwest National Lab)*
- **Sixth Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2016)** 1873
  Long Lu *(Stony Brook University)*, Mohammad Mannan *(Concordia University)*
- **Theory of Implementation Security Workshop (TIS 2016)** 1875
  Begul Bilgin, Svetla Nikova, Vincent Rijmen *(KU Leuven)*
- **WISCS'16: The 3rd ACM Workshop on Information Sharing and Collaborative Security** 1877
  Florian Kerschbaum *(SAP)*, Erik-Oliver Blass *(Airbus Group Innovations)*,
  Tomas Sander *(Hewlett Packard Labs)*
- **15th Workshop on Privacy in the Electronic Society (WPES 2016)** 1879
  Sabrina De Capitani di Vimercati *(Universita' degli Studi di Milano)*

Post-Conference Workshops co-located with CCS 2016

- **9th International Workshop on Artificial Intelligence and Security: AISec 2016** 1881
  David Mandell Freeman *(LinkedIn Corporation)*, Katerina Mitrokotsa *(Chalmers University of Technology)*,
  Arunesh Sinha *(University of Michigan)*
- **CCSW'16: 8th ACM Cloud Computing Security Workshop** 1882
  Elli Androulaki *(IBM Research)*, Michael K. Reiter *(University of North Carolina at Chapel Hill)*
- **Second Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC'16)** 1884
  Alvaro A. Cárdenas *(University of Texas, Dallas)*, Rakesh B. Bobba *(Oregon State University)*
- **2nd International Workshop on Software Protection: SPRO 2016** 1886
  Brecht Wyseur *(Nagravision S.A.)*, Bjorn De Sutter *(Ghent University)*
- **Sixth International Workshop on Trustworthy Embedded Devices (TrustED 2016)** 1888
  Xinxin Fan *(Robert Bosch LLC)*, Tim Güneysu *(University of Bremen & DFKI)*
- **MIST 2016: 8th International Workshop on Managing Insider Security Threats** 1890
  Ilsun You *(Soonchunhyang Univedrsity)*, Elisa Bertino *(Purdue University)*

Author Index 1892

CCS 2016 Conference Organization

General Chairs:	Edgar Weippl *(SBA Research, Austria)*
	Stefan Katzenbeisser *(TU Darmstadt, CYSEC, Germany)*
Program co-Chair:	Christopher Kruegel *(University of California, Santa Barbara, USA)*
	Andrew Myers *(Cornell University, USA)*
	Shai Halevi *(IBM Research, USA)*
Workshop co-Chairs:	Mathias Payer *(Purdue University, USA)*
	Stefan Mangard *(IAIK TU Graz, Austria)*
Tutorial co-Chairs:	Frederik Armknecht *(University Mannheim, Germany)*
	Gregory Neven *(IBM Zurich Research Laboratory, Switzerland)*
Poster/Demo co-Chairs:	Andreas Peter *(University of Twente, The Netherlands)*
	Dominique Schröder *(Saarland University, Germany)*
	Aniket Kate *(Purdue University, USA)*
Panel Chair:	Ahmad-Reza Sadeghi *(TU Darmstadt, CYSEC, Germany)*
Student Travel Grant co-Chairs:	Hasan Takabi *(University of North Texas, USA)*
	Stefan Brunthaler *(SBA Research, Austria)*
Publicity co-Chair:	Mauro Conti *(University of Padua, Italy)*
	Anja Lehmann *(IBM Research Zurich, Switzerland)*
	Giovanni Livraga *(Università degli Studi di Milano, Italy)*
Sponsor/Industry Outreach:	Florian Kerschbaum *(SAP, Germany)*
Social Media Chair:	Martin Schmiedecker *(SBA Research, Austria)*
Proceedings Chair:	Stefan Katzenbeisser *(TU Darmstadt, CYSEC, Germany)*
Head of Organization:	Yvonne Poul *(SBA Research, Austria)*
Steering Committee Chair:	Somesh Jha *(University of Wisconsin, Madison, USA)*
Steering Committee:	Helen Wang *(Microsoft Research, USA)*
	Carl Landwehr *(George Washington University, USA)*
	Giovanni Vigna *(University of California, Santa Barbara, USA)*
	George Danezis *(University College London, UK)*
	Trent Jaeger *(*SIGSAC Chair*) (Pennsylvania State University, USA)*
	Stefan Savage *(University of California, San Diego, USA)*
	David Basin *(ETH Zurich, Switzerland)*

Program Committee: Shweta Agrawal *(Indian Institute of Technology, India)*
Gail-Joon Ahn *(Arizona State University, USA)*
Martin Albrecht *(Royal Holloway, University of London, UK)*
Manos Antonakakis *(Georgia Institute of Technology, USA)*
Frederik Armknecht *(University of Mannheim, Germany)*
Erman Ayday *(Bilkent University, Turkey)*
Michael Backes *(CISPA*, *Saarland University & MPI-SWS, Germany)*
Davide Balzarotti *(Eurecom, Austria)*
Karthikeyan Bhargavan *(INRIA, France)*
Alex Biryukov *(University of Luxembourg, Luxembourg)*
Marina Blanton *(University of Notre Dame, France)*
Alexandra Boldyreva *(Georgia Institute of Technology, USA)*
Herbert Bos *(Vrije Universiteit / VU University Amsterdam, Netherlands)*
Elie Bursztein *(Google, USA)*
Kevin Butler *(University of Florida, USA)*
Juan Caballero *(IMDEA Software Institute, Spain)*
Yinzhi Cao *(Lehigh University, USA)*
Srdjan Capkun *(ETH Zurich, Switzerland)*
David Cash *(Rutgers University, USA)*
Lorenzo Cavallaro *(Royal Holloway, University of London, UK)*
Yan Chen *(Northwestern University, USA)*
Alessandro Chiesa *(UC Berkeley, USA)*
Yung Ryn *(*Elisha*)* Choe *(Sandia National Laboratories, USA)*
Omar Chowdhury *(Purdue University, USA)*
Véronique Cortier *(CNRS, France)*
Dana Dachman-Soled *(University of Maryland, USA)*
George Danezis *(University College London, UK)*
Anupam Datta *(Carnegie Mellon University, USA)*
Alexander De Luca *(Google, USA)*
Rinku Dewri *(University of Denver, USA)*
Adam Doupé *(Arizona State University, USA)*
Tudor Dumitras *(University of Maryland, USA)*
Stefan Dziembowski *(University of Warsaw, Poland)*
Manuel Egele *(Boston University, USA)*
William Enck *(North Carolina State University, USA)*
Dario Fiore *(IMDEA Software Institute, Spain)*
Michael Franz *(University of California, USA)*
Matt Fredrikson *(Carnegie Mellon, USA)*
Xinwen Fu *(University of Massachusetts Lowell, USA)*
Vinod Ganapathy *(Rutgers University, USA)*
Juan Garay *(Yahoo Labs, USA)*
Deepak Garg *(Max Planck Institute for Software Systems, Germany)*
Cristiano Giuffrida *(VU University Amsterdam, Netherlands)*

Program Committee (continued):

Ian Goldberg *(University of Waterloo, Canada)*
Zhongshu Gu *(IBM T.J. Watson Research Center, USA)*
Amir Herzberg *(Bar Ilan University, Israel)*
Viet Tung Hoang *(University of California, USA)*
Thorsten Holz *(Ruhr-University Bochum, Germany)*
Amir Houmansadr *(University of Massachusetts Amherst, USA)*
Yan Huang *(Indiana University, USA)*
Tibor Jager *(Ruhr-University Bochum, Germany)*
Abhishek Jain *(Johns Hopkins University, USA)*
Limin Jia *(Carnegie Mellon University, USA)*
Hongxia Jin *(Samsung Research America, USA)*
Brent Byunghoon Kang *(KAIST, South Korea)*
Chris Kanich *(University of Illinois at Chicago, USA)*
Stefan Katzenbeisser *(TU Darmstadt, CYSEC, Germany)*
Florian Kerschbaum *(SAP, Germany)*
Dmitry Khovratovich *(University of Luxembourg, Luxembourg)*
Taesoo Kim *(Georgia Tech, USA)*
Engin Kirda *(Northeastern University, USA)*
Markulf Kohlweiss *(Microsoft Research, UK)*
Vladimir Kolesnikov *(Bell Labs, USA)*
Ralf Kuesters *(University of Trier, Germany)*
Ranjit Kumaresan *(MIT, USA)*
Andrea Lanzi *(University of Milan, Italy)*
Peeter Laud *(Cybernetica AS, Estonia)*
Wenke Lee *(Georgia Institute of Technology, USA)*
Anja Lehmann *(IBM Research – Zurich, Switzerland)*
Zhou Li *(RSA Labs, UK)*
Zhenkai Liang *(National University of Singapore, Singapore)*
Benoît Libert *(ENS de Lyon, France)*
Zhiqiang Lin *(University of Texas at Dallas, USA)*
Yao Liu *(University of South Florida, USA)*
Ben Livshits *(Microsoft Research, USA)*
Long Lu *(Stony Brook University, USA)*
Matteo Maffei *(CISPA, Saarland University, Germany)*
Tal Malkin *(Columbia University, USA)*
Mohammad Mannan *(Concordia University, Canada)*
Sarah Meiklejohn *(University College London, UK)*
Prateek Mittal *(Princeton University, USA)*
Ian Molloy *(IBM Research, USA)*
Steven Murdoch *(University College London, UK)*
Arvind Narayanan *(Princeton University, USA)*
Nick Nikiforakis *(Stony Brook University, USA)*
Hamed Okhravi *(MIT Lincoln Laboratory, USA)*
Claudio Orlandi *(Aarhus University, Denmark)*
Xinming Ou *(University of South Florida, USA)*

Program Committee (continued):

Charalampos Papamanthou *(University of Maryland, USA)*
Bryan Parno *(Microsoft Research, USA)*
Mathias Payer *(Purdue University, USA)*
Roberto Perdisci *(University of Georgia, USA)*
Adrian Perrig *(ETH Zurich, Switzerland)*
Marco Pistoia *(IBM T. J. Watson Research Center, USA)*
Michalis Polychronakis *(Stony Brook University, USA)*
Raluca Ada Popa *(UC Berkeley, USA)*
Christina Pöpper *(New York University Abu Dhabi, UAE)*
Emmanuel Prouff *(ANSSI, France)*
Zhiyun Qian *(University of California, USA)*
Kui Ren *(State University of New York at Buffalo, USA)*
Konrad Rieck *(Technische Universität Braunschweig, Germany)*
William Robertson *(Northeastern University, USA)*
Alejandro Russo *(Chalmers University of Technology, Sweden)*
Andrei Sabelfeld *(Chalmers University of Technology, Sweden)*
Ahmad-Reza Sadeghi *(Technische Universität Darmstadt, Germany)*
Nitesh Saxena *(University of Alabama at Birmingham, USA)*
Jörg Schwenk *(Ruhr University Bochum, Germany)*
Abhi Shelat *(University of Virginia, USA)*
Elaine Shi *(Cornell, USA)*
Tom Shrimpton *(University of Florida, USA)*
Kapil Singh *(IBM Research, USA)*
Sooel Son *(Google, USA)*
Douglas Stebila *(McMaster University, Canada)*
Gianluca Stringhini *(University College London, UK)*
Thorsten Strufe *(TU Dresden, Germany)*
Ed Suh *(Cornell University, USA)*
Kun Sun *(College of William and Mary, USA)*
Jakub Szefer *(Yale University, USA)*
Gang Tan *(Pennsylvania State University, USA)*
Stefano Tessaro *(University of California, USA)*
Mohit Tiwari *(UT Austin, USA)*
Nikos Triandopoulos *(Boston University, USA)*
Mahesh Tripunitara *(University of Waterloo, Canada)*
XiaoFeng Wang *(Indiana University, USA)*
Zhi Wang *(Florida State University, USA)*
Hoeteck Wee *(ENS, France)*
Edgar Weippl *(SBA Research, Austria)*
Wenyuan Xu *(University of South Carolina & Zhejiang University, USA/China)*
Dongyan Xu *(Purdue University, USA)*
Danfeng Daphne Yao *(Virginia Tech, USA)*
Ting Yu *(Qatar Computing Research Institute, Qatar)*
David Zage *(Intel corporation, USA)*

Program Committee (continued):

Yanchao Zhang *(Arizona State University, USA)*
Kehuan Zhang *(The Chinese University of Hong Kong, Hong Kong)*
Yinqian Zhang *(The Ohio State University, USA)*
Xiangyu Zhang *(Purdue University, USA)*
Sheng Zhong *(Nanjing University, China)*
Haojin Zhu *(Shanghai Jiao Tong University, China)*

Poster / Demo Program Committee:

David Barrera *(ETH Zurich, Switzerland)*
Lejla Batina *(Radboud University Nijmegen, Netherlands)*
Jeremiah Blocki *(Purdue University, USA)*
Christina Brzuska *(Hamburg University of Technology, Germany)*
Sven Bugiel *(Saarland University, Germany)*
Thomas Eisenbarth *(Worcester Polytechnic Institute, USA)*
Byoungyoung Lee *(Georgia Institute of Technology, USA)*
Andrew Miller *(University of Illinois at Urbanan-Champaign, USA)*
Muhammad Naveed *(University of Southern California, USA)*
Olya Ohrimenko *(Microsoft Research Cambridge, UK)*
Raphael Reischuk *(ETH Zürich, Switzerland)*
Giancarlo Pellegrino *(Saarland University, Germany)*
Erik Tews *(University of Birmingham, UK)*

Additional reviewers:

Michel Abdalla
Hamza Abusalah
Ghada Almashaqbeh
Abhishek Anand
Dennis Andriesse
Elli Androulaki
George Argyros
Cornelius Aschermann
Gilad Asharov
Daniele Asoni
Nuttapong Attrapadung
Jean-Philippe Aumasson
Sarah Azouvi
Steve Babbage
Saikrishna Badrinarayanan
Shi Bai
Xiaolong Bai
Foteini Baldimtsi
Musard Balliu
Adam Bates
Erick Bauman
Jethro Beekman
Iddo Bentov
Pascal Berrang
Arjun Bhagoji
Rohit Bhatia
Sanjay Bhattacherjee
Nataliia Bielova
Battista Biggio
Vincent Bindschaedler
Cecylia Bocovich
Tobias Boelter
Joseph Bonneau
Yazan Boshmaf
Ioana Boureanu
Florian Bourse
Sven Bugiel
Mark Bun
Christian Cachin
Dario Catalano
Abdelberi Chaabane
Supriyo Chakraborty
Swarup Chandra
Nishanth Chandran
Rahul Chatterjee
Jie Chen
Jiongyi Chen
Kai Chen

Additional reviewers (continued):

Yimin Chen
Yue Chen
Rui Chen
Xi Chen
Nathan Chenette
Yushi Cheng
Vincent Cheval
ChangHo Choi
Seung Geol Choi
Sung Choi
Zheng Leong Chua
Laurent Chuat
Simon Chung
Jeremy Clark
Lucian Cojocar
Moritz Contag
Scott Coull
Cas Cremers
Paolo D'Arco
Santanu, K Dash
Amit Datta
Bernardo David
Xavier de Carné de Carnavalet
Jean Paul Degabriele
Antoine Delignat-Lavaud
Ioannis Demertzis
Soteris Demetriou
Wenrui Diao
Yu Ding
Daniel Dinu
Natnatee Dokmai
Benjamin Dowling
Evan Downing
Jannik Dreier
Manu Drijvers
Ruian Duan
Sevtap Duman
Annie Edmundson
Mohamed El Massad
Leo Fan
Serge Fehr
Ben A. Fisch
Christopher Fletcher
Yangchun Fu
Chaya Ganesh
Peng Gao
Xing Gao
Romain Gay
Nethanel Gelernter
Rosario Gennaro
Craig Gentry
Martin Georgiev
Esha Ghosh
Yossi Gilad
Esha Gosh
Matthew Green
Johann Großschädl
Bei Guan
Eric Gustafson
Tzipora Halevi
Daniel Hausknecht
Boyuan He
Daniel Hedin
Scott Heidbrink
Grant Hernandez
Alejandro Hevia
Andrei Homescu
Hongxin Hu
Heqing Huang
Moses Ike
DaeHee Jang
Jinsoo Jang
Kai Jansen
Angela Jäschke
Yaoqi Jia
Xiaocong Jin
David Johnston
Zach Jorgensen
Aljosha Judmayer
Yuan Kang
Vishal Karande
Shiva Kasiviswanathan
Omer Katz
Mehmet Kayaalp
Issa Khalil
Sheharbano Khattak
Dakshita Khurana
Chunghwan Kim
Gihyuk Ko
Katharina Kohls
Deguang Kong
Koen Koning

Additional reviewers (continued):

Radesh Konoth
Ahmed Kosba
Lucas Kowalczyk
Mukul Kulkarni
Yonghwi Kwon
Fabien Laguillaumie
Kim Laine
Enrique Larraia de Vega
Per Larsen
Sven Laur
Hojoon Lee
Tae-Ho Lee
Yeonjoon Lee
Lingguang Lei
Hemi Leibowitz
Xue Leng
Tancrède Lepoint
Chaohao Li
Tao Li
Tongxin Li
Zhen Ling
Chang Liu
Rui Liu
Shen Liu
Xiangyu Liu
Vadim Lyubashevsky
Olaf Maennel
Christian Mainka
Daniel Malinowski
Alex Malozemoff
Andrea Mambretti
Praveen Manoharan
Mark Manulis
Jian Mao
Piotr Mardziel
Ali Mashtizadeh
Steve Matsumoto
Keith Mayes
David McCann
Wei Meng
Georg Merzdovnik
Peihan Miao
Eric Miles
Pratyush Mishra
Aikaterini Mitrokotsa
Vladislav Mladenov
Tarik Moataz
Hooman Mohajeri
Manar Mohamed
Hart Montgomery
Fabrice Mouhartem
Johannes Müller
Michael Naehrig
Muhammad Naveed
Kartik Nayak
Ajaya Neupane
Ryo Nishimaki
Ilia Nouretdinov
Olga Ohrimenko
Aggelos Oikonomopoulos
Mark O'Neill
Jiaxin Pan
Xiang Pan
Xiaorui Pan
Giorgios Panagiotakos
Andriy Panchenko
Alisa Pankova
Dimitrios Papadopoulos
Chris Pappas
Raúl Pardo
Sunoo Park
Valerio Pastro
Kenneth G. Paterson
Andre Pawlowski
Chris Peikert
Léo Paul Perrin
Thomas Peters
Theofilos Petsios
Martin Pettai
Van-Thuan Pham
Krzysztof Pietrzak
Rishabh Poddar
Bertram Poettering
Pille Pullonen
Ivan Pustogarov
Chengxiong Qian
Zhan Qin
Zhengyang Qu
Srinivasan Raghuraman
Somindu Ramanna

Additional reviewers (continued):

Daniel Rausch
Sanjay Rawat
Baishakhi Ray
Mariana Raykova
Bradley Reaves
Raphael Reischuk
Ling Ren
Guénaël Renault
Thomas Ristenpart
Ben Riva
Pankaj Rohatgi
Mike Rosulek
Tim Ruffing
Scott Ruoti
David Rupprecht
Teemu Rytilahti
Brendan Saltaformaggio
Takayuki Sasaki
Karla Saur
Alessandra Scafuro
Guillaume Scerri
Falk Schellenberg
Benedikt Schmidt
Daniel Schoepe
Adam Sealfon
Jean-Pierre Seifert
Shayak Sen
Aria Shahverdi
Aria Shahverdi
Kumar Sharad
Mahmood Sharif
Wenbo Shen
Yilin Shen
SeungWon Shin
Maliheh Shirvanian
Prakash Shrestha
Haya Shulman
Alexander Sjösten
Nigel Smart
Juraj Somorovsky
Chengyu Song
Libin Song
Máté Soos
Aikaterini Sotiraki
Radu State

Ben Stock
Guillermo Suarez-Tangil
Octavian Suciu
Nick Sullivan
Nik Sultana
Jingchao Sun
Yixin Sun
Adrian Tang
Di Tang
Qiang Tang
Aishwarya Thiruvengadam
Kurt Thomas
Dave Tian
Jing Tian
Yuan Tian
Alin Tomescu
Ni Trieu
Roberto Trifiletti
Tomasz Truderung
Michael Tschantz
Aleksei Udovenko
Johanna Ullrich
Steven Van Acker
Bart van Delft
Erik Van der Kouwe
Victor Van der Veen
Giorgos Vasiliadis
Marco Vassena
Fre Vercauteren
Damien Vergnaud
Stijn Volckaert
Emanuel von Zezschwitz
Artemios Voyiatzis
Shengye Wan
Frank Wang
Huibo Wang
Ruowen Wang
Shuai Wang
Tao Wang
Weihang Wang
Weiren Wang
Xiao Wang
Fengguo Wei
Michael Weissbacher
Douglas Wikström

Additional reviewers (continued):

Jan Willemson
Maverick Woo
Christian Wressnegger
David Wu
Tao Xiang
Xiaokui Xiao
Yuan Xiao
Haitao Xu
Chen Yan
Ziqi Yang
Xin Yao
Quanqi Ye
Yinbo Yu
Kan Yuan
Qinggang Yue
Thomas Zacharias
Samee Zahur
Santiago Zanella-Beguelin
Greg Zaverucha
Dongrui Zeng
Cong Zhang
Jialong Zhang
Nan Zhang
Ning Zhang
Rui Zhang
Su Zhang
Taiming Zhang
Tianwei Zhang
Xiaokuan Zhang
Yupeng Zhang
Lianying Zhao
Wenting Zheng
Hong-Sheng Zhou
Xinyan Zhou
Zhe Zhou
Tiantian Zhu
Ziyun Zhu
Dionysis Zindros
Chaoshun Zuo

CCS 2016 Sponsor & Supporters

Sponsor:	acm SIGSAC	
Platinum Supporters:	NSF	SBA Research
Gold Supporters:	CISCO	HUAWEI
	Bai du 百度	
Silver Supporters:	IBM Research	Office of Naval Research ONR Science & Technology
	Hewlett Packard Enterprise	BOSCH
Bronze Supporters:	Google	SAP®
	cyan SECURITY GROUP	