October 15-19, 2018
Toronto, ON, Canada

Association for Computing Machinery

Advancing Computing as a Science & Profession

CCS'18

Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security

Sponsored by:

ACM SIGSAC

General Chairs:

David Lie (University of Toronto)
Mohammad Mannan (Concordia University)

Program Chairs:

Michael Backes (CISPA Helmholtz Center i.G.)
XiaoFeng Wang (Indiana University)

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 © 2018 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: 978-1-4503-5693-0

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

General Chairs' Welcome

Welcome to the 2018 ACM Conference on Computer and Communications Security! We are delighted to organize the first ACM CCS in Canada, the flagship annual conference of ACM's Special Interest Group on Security, Audit and Control (SIGSAC). Since 1993, CCS has brought together world's leading information security researchers and practitioners to this annual scientific event of exciting results in security and privacy. We are very happy to welcome you all in Toronto, one of the most diverse, multicultural and cosmopolitan cities in the world---a genuine representation of Canada, including its aboriginals, immigrants and refugees.

This year's main program includes 134 high quality research papers, accepted from 809 submissions. In addition, there are 12 co-located workshops covering emerging topics in security and privacy, four tutorials, one panel, and two exciting keynotes from Helen Nissenbaum and Shai Halevi. Together, this will make ACM CCS one of the largest academic security conferences in 2018.

We have a long list of people to thank. First and foremost, the authors of all submitted and accepted papers in the main conference and the workshops—without their dedication to the quest for knowledge and scientific inquiry, we could not have such a high standard technical program. We furthermore want to thank the CCS Program Committee members and the PC Chairs, for their time and commitment in the peer review process and selecting the most pertinent and interesting papers from the submissions. We would also like to thank the Organizing and Steering Committee members, who spent numerous hours behind the scenes to have a smooth program. Last but not the least, we want to thank CCS 2018 sponsors for their generous financial support, and ACM officials for their help over the year in organizing such a large event.

We hope that ACM CCS 2018 will be a memorable experience for you, providing you with unique opportunities to learn state-of-the-art advancement in security and privacy, to share ideas with other attendees from around the world, and to inspire novel ideas for understanding and solving security issues affecting the global citizens.

We wish your stay in Toronto to be a pleasant and enjoyable one!

David Lie
ACM CCS 2018 General Co-chair
University of Toronto

Mohammad Mannan
ACM CCS 2018 General Co-chair
Concordia University

Program Chairs' Welcome

As the ACM's flagship security and privacy conference for more than two decades and the world's largest forum on computing and communications security research, CCS today is facing great challenges in meeting the demands of an expanding community and also ensuring high quality of its published research. This year's conference is unique as the last one before the conference's model change, moving from a single deadline toward a multiple deadline and more journal-like system.

This year, a total of 809 submissions were received by the conference. Among them, 134 were selected to appear in the program and be included in the proceedings, with an acceptance rate of 16.6%. These papers were reviewed by a Program Committee of 159 security and privacy experts from academia, industry and government around the world. Following the convention in the past years, the review process includes three rounds. Each submission were reviewed by two PC members in the first round and those moving to the later rounds received additional reviews, depending on the results of the initial reviews. The vast majority of the accepted papers have 4 to 5 reviews. Right after the second round, authors were given the opportunities to respond to the reviews received. During the final review stage, papers were extensively discussed online, taking into account both reviews and the author responses, and additional reviews were assigned to those controversial or with low confident reviews only. Like last year, we used Toronto Paper Matching System (TPMS) to automatically assign papers and then manually adjusted the assignments when necessary. Most PC members have reviewed 16 to 20 papers.

The accepted papers cover a large spectrum of security and privacy topics, ranging from cryptography and formal methods to SDN, blockchain and IoT security. This diversity demonstrates the breadth of applied security and privacy research and also reflects the technological trends in the area.

This year's CCS has returned to the two PC chair rotation system. To help manage the large number of submissions, 6 area chairs were invited to assist the PC chairs in handling the submissions in their individual areas, advising the paper discussion process and selecting papers. They also participated in selection of award papers. We thank the area chairs and all other PC members and external reviewers for their hard work and for their professionalism. We are also grateful to the General Chair, David Lie and Mohammad Mannan for taking care of other issues that make the conference possible, and to the Proceedings Chairs, Aniket Kate and Ryan Henry for working with the publisher to produce the proceedings, and to Ben Stock and Xueqiang Wang for managing the submission and paper assignment systems, and to all the authors for submitting to CCS.

Enjoy the conference!

Michael Backes
CISPA Helmholtz Center I.G.

XiaoFeng Wang
Indiana University, Bloomington

Table of Contents

ACM CCS 2018 Conference Organization xx

ACM CCS 2018 Sponsor & Patrons xxviii

Session: Keynote Talk I

- **Achieving Meaningful Privacy in Digital Systems** 1
  Helen Nissenbaum *(Cornell Tech)*

Session 1A: SDN 1

Session Chair: Brad Reaves *(North Carolina State University)*

- **Towards Fine-grained Network Security Forensics and Diagnosis in the SDN Era** 3
  Haopei Wang, Guangliang Yang, Phakpoom Chinprutthiwong, Lei Xu, Yangyong Zhang, Guofei Gu *(Texas A&M University)*
- **vNIDS: Towards Elastic Security with Safe and Efficient Virtualization of Network Intrusion Detection Systems** 17
  Hongda Li, Hongxin Hu *(Clemson University)*, Guofei Gu *(Texas A&M University)*, Gail-Joon Ahn *(Arizona State University)*, Fuqiang Zhang *(Clemson University)*

Session 1B: Privacy

Session Chair: Apu Kapadia *(Indiana University)*

- **ABY^3: A Mixed Protocol Framework for Machine Learning** 35
  Payman Mohassel, Peter Rindal *(Visa)*
- **Voting: You Can't Have Privacy without Individual Verifiability** 53
  Véronique Cortier *(CNRS & Loria)*, Joseph Lallemand *(Inria & Loria)*

Session 1C: Smart Contracts

Session Chair: Yan Chen *(Northwestern University)*

- **Securify: Practical Security Analysis of Smart Contracts** 67
  Petar Tsankov, Andrei Dan, Dana Drachsler-Cohen *(ETH Zurich)*, Arthur Gervais *(Imperial College London)*, Florian Bünzli, Martin Vechev *(ETH Zurich)*
- **BitML: A Calculus for Bitcoin Smart Contracts** 83
  Massimo Bartoletti *(University of Cagliari)*, Roberto Zunino *(University of Trento)*

Session 1D: ML for Deanonymization

Session Chair: Nikita Borisov *(Universiy of Illinois at Urbana-Champaign)*

- **Large-Scale and Language-Oblivious Code Authorship Identification** 101
  Mohammed Abuhamad, Tamer AbuHmed *(Inha University)*, Aziz Mohaisen *(University of Central Florida)*, DaeHun Nyang *(Inha University)*
- **Fraud De-Anonymization for Fun and Profit** 115
  Nestor Hernandez, Mizanur Rahman, Ruben Recabarren, Bogdan Carbunar *(Florida International University)*

Session 2A: Side Channel 1

Session Chair: Fengwei Zhang *(Wayne State University)*

- **Unveiling Hardware-based Data Prefetcher, a Hidden Source of Information Leakage** 131
  Youngjoo Shin *(Kwangwoon University)*, Hyung Chan Kim, Dokeun Kwon, Ji Hoon Jeong *(The Affiliated Institute of ETRI)*, Junbeom Hur *(Korea University)*
- **Ohm's Law in Data Centers: A Voltage Side Channel for Timing Power Attacks** 146
  Mohammad A. Islam, Shaolei Ren *(University of California, Riverside)*

- **Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers** 163
  Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, Aurélien Francillon *(EURECOM)*
- **Nemesis: Studying Microarchitectural Timing Leaks in Rudimentary CPU Interrupt Logic** .. 178
  Jo Van Bulck, Frank Piessens, Raoul Strackx *(imec-DistriNet, KU Leuven)*

Session 2B: Differential Privacy 1

Session Chair: Nikita Borisov *(Universiy of Illinois at Urbana-Champaign)*

- **Utility-Aware Synthesis of Differentially Private and Attack-Resilient Location Traces** 196
  Mehmet Emre Gursoy, Ling Liu, Stacey Truex, Lei Yu, Wenqi Wei *(Georgia Institute of Technology)*
- **CALM: Consistent Adaptive Local Marginal for Marginal Release under Local Differential Privacy** 212
  Zhikun Zhang *(Zhejiang University & Purdue University)*,
  Tianhao Wang, Ninghui Li, Shibo He, Jiming Chen *(Zhejiang University)*
- **MVG Mechanism: Differential Privacy under Matrix-Valued Query** 230
  Thee Chanyaswad, Alex Dytso, H. Vincent Poor, Prateek Mittal *(Princeton University)*
- **Tight on Budget? Tight Bounds for r-Fold Approximate Differential Privacy** 247
  Sebastian Meiser *(University College London)*, Esfandiar Mohammadi *(ETH Zurich)*

Session 2C: Crypto Attacks

Session Chair: Cas Cremers *(CISPA Helmholtz Center i.G.)*

- **Practical State Recovery Attacks against Legacy RNG Implementations** 265
  Shaanan N. Cohney *(University of Pennsylvania)*, Matthew D. Green *(Johns Hopkins University)*,
  Nadia Heninger *(University of Pennsylvania)*
- **Prime and Prejudice: Primality Testing Under Adversarial Conditions** 281
  Martin R. Albrecht, Jake Massimo, Kenneth G. Paterson *(Royal Holloway, University of London)*,
  Juraj Somorovsky *(Ruhr University Bochum)*
- **Release the Kraken: New KRACKs in the 802.11 Standard** 299
  Mathy Vanhoef, Frank Piessens *(imec-DistriNet, KU Leuven)*
- **Pump up the Volume: Practical Database Reconstruction from Volume Leakage on Range Queries** 315
  Paul Grubbs *(Cornell University)*,
  Marie-Sarah Lacharié, Brice Minaud, Kenneth G. Paterson *(Royal Holloway, University of London)*

Session 2D: ML 2

Session Chair: Battista Biggio *(University of Cagliari, Italy)*

- **Yet Another Text Captcha Solver: A Generative Adversarial Network Based Approach** 332
  Guixin Ye, Zhanyong Tang, Dingyi Fang *(Northwest University)*,
  Zhanxing Zhu, Yansong Feng *(Peking University)*,
  Pengfei Xu, Xiaojiang Chen *(Northwest University)*, Zheng Wang *(Lancaster University)*
- **Model-Reuse Attacks on Deep Learning Systems** 349
  Yujie Ji, Xinyang Zhang *(Lehigh University)*, Shouling Ji *(Zhejiang University)*,
  Xiapu Luo *(Hong Kong Polytechnic University)*, Ting Wang *(Lehigh University)*
- **LEMNA: Explaining Deep Learning based Security Applications** 364
  Wenbo Guo *(Pennsylvania State University & JD Security Research Center)*,
  Dongliang Mu *(Nanjing University & Pennsylvania State University)*,
  Jun Xu *(Stevens Institute of Technology & Pennsylvania State University)*,
  Purui Su *(Chinese Academy of Sciences)*, Gang Wang *(Virginia Tech)*,
  Xinyu Xing *(Pennsylvania State University & JD Security Research Center)*
- **Effective Program Debloating via Reinforcement Learning** 380
  Kihong Heo *(University of Pennsylvania)*, Woosuk Lee *(University of Pennsylvania & Hanyang University)*,
  Pardis Pashakhanloo, Mayur Naik *(University of Pennsylvania)*

Session 3A: Binary Analysis

Session Chair: Stefan Nürnberger *(CISPA Helmholtz Center i.G.)*

- **Towards Paving the Way for Large-Scale Windows Malware Analysis: Generic Binary Unpacking with Orders-of-Magnitude Performance Boost** 395
  Binlin Cheng *(Wuhan University & Hubei Normal University)*, Jiang Ming *(University of Texas at Arlington)*, Jianming Fu, Guojun Peng *(Wuhan University)*, Ting Chen, Xiaosong Zhang *(University of Electronic Science and Technology of China)*, Jean-Yves Marion *(Université de Lorraine)*
- **K-Hunt: Pinpointing Insecure Cryptographic Keys from Execution Traces** 412
  Juanru Li *(Shanghai Jiao Tong University)*, Zhiqiang Lin *(The Ohio State University)*, Juan Caballero *(IMDEA Software Institute)*, Yuanyuan Zhang, Dawu Gu *(Shanghai Jiao Tong University)*
- **Using Logic Programming to Recover C++ Classes and Methods from Compiled Executables** 426
  Edward J. Schwartz, Cory F. Cohen, Michael Duggan, Jeffrey Gennari, Jeffrey S. Havrilla, Charles Hines *(Carnegie Mellon University)*
- **VMHunt: A Verifiable Approach to Partially-Virtualized Binary Code Simplification** 442
  Dongpeng Xu *(Pennsylvania State University)*, Jiang Ming *(University of Texas at Arlington)*, Yu Fu, Dinghao Wu *(Pennsylvania State University)*

Session 3B: Differential Privacy 2

Session Chair: Gilles Barthe *(IMDEA Software Institute)*

- **Preserving Both Privacy and Utility in Network Trace Anonymization** 459
  Meisam Mohammady, Lingyu Wang *(Concordia University)*, Yuan Hong *(Illinois Institute of Technology)*, Habib Louafi, Makan Pourzandi *(Ericsson Research Security)*, Mourad Debbabi *(Concordia University)*
- **Detecting Violations of Differential Privacy** 475
  Zeyu Ding, Yuxin Wang, Guanhong Wang, Danfeng Zhang, Daniel Kifer *(Pennsylvania State University)*
- **Secure Computation with Differentially Private Access Patterns** 490
  Sahar Mazloom, S. Dov Gordon *(George Mason University)*
- **DP-Finder: Finding Differential Privacy Violations by Sampling and Optimization** 508
  Benjamin Bichsel, Timon Gehr, Dana Drachsler-Cohen, Petar Tsankov, Martin Vechev *(ETH Zurich)*

Session 3C: Crypto: Lattice/ZKP

Session Chair: Yan Huang *(Indiana University)*

- **Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures** 525
  Jonathan Katz *(University of Maryland)*, Vladimir Kolesnikov *(Georgia Institute of Technology)*, Xiao Wang *(University of Maryland)*
- **Symbolic Proofs for Lattice-Based Cryptography** 538
  Gilles Barthe *(IMDEA Software Institute)*, Xiong Fan, Joshua Gancher *(Cornell University)*, Benjamin Grégoire *(INRIA)*, Charlie Jacomme *(LSV & CNRS & ENS Paris-Saclay & INRIA & Université Paris-Saclay)*, Elaine Shi *(Cornell University)*
- **Lattice-Based zk-SNARKs from Square Span Programs** 556
  Rosario Gennaro *(City College of New York)*, Michele Minelli, Anca Nitulescu, Michele Orrù *(École Normale Supérieure)*
- **Lattice-Based Group Signatures and Zero-Knowledge Proofs of Automorphism Stability** 574
  Rafael del Pino *(ENS Paris)*, Vadim Lyubashevsky, Gregor Seiler *(IBM Research - Zurich)*

Session 3D: ML 3

Session Chair: Neil Gong *(Iowa State University)*

- **Tiresias: Predicting Security Events Through Deep Learning** 592
  Yun Shen *(Symantec)*, Enrico Mariconti *(University College London)*, Pierre Antoine Vervier *(Symantec)*, Gianluca Stringhini *(Boston University)*

- **DeepMem: Learning Graph Neural Network Models for Fast and Robust Memory Forensic Analysis** 606
  Wei Song, Heng Yin *(University of California, Riverside)*,
  Chang Liu, Dawn Song *(University of California, Berkeley)*
- **Property Inference Attacks on Fully Connected Neural Networks using Permutation Invariant Representations** 619
  Karan Ganju, Qi Wang *(University of Illinois at Urbana-Champaign)*, Wei Yang *(University of Texas at Dallas)*,
  Carl A. Gunter, Nikita Borisov *(University of Illinois at Urbana-Champaign)*
- **Machine Learning with Membership Privacy using Adversarial Regularization** 634
  Milad Nasr *(University of Massachusetts, Amherst)*, Reza Shokri *(National University of Singapore)*,
  Amir Houmansadr *(University of Massachusetts, Amherst)*

Session: Keynote Talk II

- **Advanced Cryptography: Promise and Challenges** 647
  Shai Halevi *(IBM Research)*

Session 4A: SDN 2

Session Chair: Brad Reaves *(NC State University)*

- **Cross-App Poisoning in Software-Defined Networking** 648
  Benjamin E. Ujcich *(University of Illinois at Urbana-Champaign)*, Samuel Jero *(MIT Lincoln Laboratory)*,
  Anne Edmundson *(Princeton University)*, Qi Wang *(University of Illinois at Urbana-Champaign)*,
  Richard Skowyra, James Landry *(MIT Lincoln Laboratory)*,
  Adam Bates, William H. Sanders *(University of Illinois at Urbana-Champaign)*,
  Cristina Nita-Rotaru *(Northeastern University)*, Hamed Okhravi *(MIT Lincoln Laboratory)*
- **AIM-SDN: Attacking Information Mismanagement in SDN-datastores** 664
  Vaibhav Hemant Dixit, Adam Doupé, Yan Shoshitaishvili, Ziming Zhao *(Arizona State University)*,
  Gail-Joon Ahn *(Arizona State University & Samsung Research)*

Session 4B: SecComp 1

Session Chair: Jonathan Katz *(UMD)*

- **Fast Secure Computation for Small Population over the Internet** 677
  Megha Byali, Arun Joseph, Arpita Patra, Divya Ravi *(Indian Institute of Science)*
- **An End-to-End System for Large Scale P2P MPC-as-a-Service and Low-Bandwidth MPC for Weak Participants** 695
  Assi Barak *(Bar-Ilan University)*, Martin Hirt *(ETH Zurich)*, Lior Koskas, Yehuda Lindell *(Bar-Ilan University)*

Session 4C: Blockchain 1

Session Chair: Rosario Gennaro *(CUNY)*

- **The Gap Game** 713
  Itay Tsabary, Ittay Eyal *(Technion)*
- **A Better Method to Analyze Blockchain Consistency** 729
  Lucianna Kiffer, Rajmohan Rajaraman, abhi shelat *(Northeastern University)*

Session 4D: Encrypted Search & Computation 1

Session Chair: Ryan Henry *(University of Calgary)*

- **Result Pattern Hiding Searchable Encryption for Conjunctive Queries** 745
  Shangqi Lai *(Monash University & Data61, CSIRO)*,
  Sikhar Patranabis *(Indian Institute of Technology Kharagpur)*, Amin Sakzad, Joseph K. Liu *(Monash University)*,
  Debdeep Mukhopadhyay *(Indian Institute of Technology Kharagpur)*,
  Ron Steinfeld *(Monash University)*, Shi-Feng Sun *(Monash University & Data61, CSIRO)*,
  Dongxi Liu *(Data61, CSIRO)*, Cong Zuo *(Monash University & Data61, CSIRO)*
- **Practical Backward-Secure Searchable Encryption from Symmetric Puncturable Encryption** 763
  Shi-Feng Sun *(Monash University & CSIRO)*,
  Xingliang Yuan, Joseph K. Liu, Ron Steinfeld, Amin Sakzad *(Monash University)*,
  Viet Vo *(Monash University & CSIRO)*, Surya Nepal *(CSIRO)*

Session 5A: Cyberphysical

Session Chair: Nils Ole Tippenhauer *(CISPA Helmholtz Center i.G.)*

- **Scission: Signal Characteristic-Based Sender Identification and Intrusion Detection in Automotive Networks** 787
  Marcel Kneib, Christopher Huth *(Robert Bosch GmbH)*
- **Detecting Attacks Against Robotic Vehicles: A Control Invariant Approach** 801
  Hongjun Choi, Wen-Chuan Lee, Yousra Aafer, Fan Fei, Zhan Tu, Xiangyu Zhang, Dongyan Xu, Xinyan Deng *(Purdue University)*
- **Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems** 817
  Wissam Aoudi *(Chalmers University of Technology)*, Mikel Iturbe *(Mondragon University)*, Magnus Almgren *(Chalmers University of Technology)*
- **On the Safety of IoT Device Physical Interaction Control** 832
  Wenbo Ding, Hongxin Hu *(Clemson University)*

Session 5B: SecComp 2

Session Chair: Kenny Paterson *(Royal Holloway)*

- **HyCC: Compilation of Hybrid Protocols for Practical Secure Computation** 847
  Niklas Büscher, Daniel Demmler, Stefan Katzenbeisser, David Kretzmer, Thomas Schneider *(Technische Universität Darmstadt)*
- **NANOPI: Extreme-Scale Actively-Secure Multi-Party Computation: Resolving the Space-Round Dilemma using Lightweight Program Instrumentation** 862
  Ruiyu Zhu *(Indiana University)*, Darion Cassel *(Carnegie Mellon University)*, Amr Sabry, Yan Huang *(Indiana University)*
- **Generalizing the SPDZ Compiler For Other Protocols** 880
  Toshinori Araki *(NEC)*, Assi Barak *(Bar-Ilan University)*, Jun Furukawa *(NEC Israel Research Center)*, Marcel Keller *(Data61)*, Yehuda Lindell *(Bar-Ilan University)*, Kazuma Ohara, Hikaru Tsuchida *(NEC)*
- **Compressing Vector OLE** 896
  Elette Boyle *(IDC)*, Geoffroy Couteau *(KIT)*, Niv Gilboa *(Ben Gurion University)*, Yuval Ishai *(Technion)*

Session 5C: Blockchain 2

Session Chair: Rosario Gennaro *(CUNY)*

- **Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability** 913
  Christian Badertscher *(ETH Zurich)*, Peter Gaži *(IOHK)*, Aggelos Kiayias *(University of Edinburgh)*, Alexander Russell *(University of Connecticut)*, Vassilis Zikas *(University of Edinburgh)*
- **RapidChain: Scaling Blockchain via Full Sharding** 931
  Mahdi Zamani *(Visa Research)*, Mahnush Movahedi *(Dfinity)*, Mariana Raykova *(Yale University)*
- **General State Channel Networks** 949
  Stefan Dziembowski *(University of Warsaw)*, Sebastian Faust, Kristina Hostáková *(TU Darmstadt)*
- **FairSwap: How To Fairly Exchange Digital Goods** 967
  Stefan Dziembowski *(University of Warsaw)*, Lisa Eckey, Sebastian Faust *(TU Darmstadt)*

Session 5D: Encrypted Search & Computation 2

Session Chair: Ryan Henry *(University of Calgary)*

- **Secure Search on Encrypted Data via Multi-Ring Sketch** 985
  Adi Akavia *(Academic College of Tel-Aviv Jaffa)*, Dan Feldman, Hayim Shaul *(University of Haifa)*
- **Private Stateful Information Retrieval** 1002
  Sarvar Patel, Giuseppe Persiano, Kevin Yeo *(Google LLC)*

- **ALCHEMY: A Language and Compiler for Homomorphic Encryption Made easY** 1020
  Eric Crockett *(University of Michigan & Georgia Institute of Technology)*,
  Chris Peikert, Chad Sharp *(University of Michigan)*
- **New Constructions for Forward and Backward Private Symmetric Searchable Encryption** 1038
  Javad Ghareh Chamani *(Hong Kong University of Science and Technology & Sharif University of Technology)*,
  Dimitrios Papadopoulos *(Hong Kong University of Science and Technology)*,
  Charalampos Papamanthou *(University of Maryland)*, Rasool Jalili *(Sharif University of Technology)*

Session 6A: IoT

Session Chair: Yuqiong Sun *(Symantec Research Labs)*

- **Situational Access Control in the Internet of Things** 1056
  Roei Schuster *(Tel Aviv University & Cornell Tech)*, Vitaly Shmatikov *(Cornell Tech)*,
  Eran Tromer *(Tel Aviv University & Columbia University)*
- **HoMonit: Monitoring Smart Home Apps from Encrypted Traffic** 1074
  Wei Zhang, Yan Meng, Yugeng Liu *(Shanghai Jiao Tong University)*,
  Xiaokuan Zhang, Yinqian Zhang *(Ohio State University)*, Haojin Zhu *(Shanghai Jiao Tong University)*
- **Pinto: Enabling Video Privacy for Commodity IoT Cameras** 1089
  Hyunwoo Yu, Jaemin Lim, Kiyeon Kim, Suk-Bok Lee *(Hanyang University)*
- **If This Then What? Controlling Flows in IoT Apps** 1102
  Iulia Bastys *(Chalmers University of Technology)*, Musard Balliu *(KTH Royal Institute of Technology)*,
  Andrei Sabelfeld *(Chalmers University of Technology)*

Session 6B: Mobile 1

Session Chair: Sven Bugiel *(CISPA Helmholtz Center i.G.)*

- **ClickShield: Are You Hiding Something? Towards Eradicating Clickjacking on Android** 1120
  Andrea Possemato *(EURECOM)*, Andrea Lanzi *(Universita' degli Studi di Milano)*,
  Simon Pak Ho Chung, Wenke Lee *(Georgia Institute of Technology)*, Yanick Fratantonio *(EURECOM)*
- ***JN-SAF*: Precise and Efficient NDK/JNI-aware Inter-language Static Analysis Framework for Security Vetting of Android Applications with Native Code** 1137
  Fengguo Wei *(University of South Florida)*,
  Xingwei Lin *(University of Electronic Science and Technology of China)*,
  Xinming Ou *(University of South Florida)*,
  Ting Chen, Xiaosong Zhang *(University of Electronic Science and Technology of China)*
- **Precise Android API Protection Mapping Derivation and Reasoning** 1151
  Yousra Aafer, Guanhong Tao *(Purdue University)*, Jianjun Huang *(Renmin University of China)*,
  Xiangyu Zhang, Ninghui Li *(Purdue University)*
- **Invetter: Locating Insecure Input Validations in Android Services** 1165
  Lei Zhang, Zhemin Yang, Yuyu He, Zhenyu Zhang *(Fudan University)*,
  Zhiyun Qian *(University of California, Riverside)*, Geng Hong, Yuan Zhang, Min Yang *(Fudan University)*

Session 6C: Crypto 3

Session Chair: Jonathan Katz *(UMD)*

- **Fast Multiparty Threshold ECDSA with Fast Trustless Setup** 1179
  Rosario Gennaro *(City University of New York)*, Steven Goldfeder *(Princeton University)*
- **On the Security of the PKCS#1 v1.5 Signature Scheme** 1195
  Tibor Jager, Saqib A. Kakvi *(Paderborn University)*, Alexander May *(Ruhr-University Bochum)*
- **Secure Outsourced Matrix Computation and Application to Neural Networks** 1209
  Xiaoqian Jiang, Miran Kim *(University of Texas, Health Science Center)*, Kristin Lauter *(Microsoft Research)*,
  Yongsoo Song *(University of California, San Diego)*
- **Labeled PSI from Fully Homomorphic Encryption with Malicious Security** 1223
  Hao Chen *(Microsoft Research)*, Zhicong Huang *(École Polytechnique Fédérale de Lausanne)*,
  Kim Laine *(Microsoft Research)*, Peter Rindal *(Oregon State University)*

Session 6D: Usable 1

Session Chair: Joshua Schiffman Schiffman *(HP Labs, HP Inc.)*

- **Asking for a Friend: Evaluating Response Biases in Security User Studies**..... 1238
  Elissa M. Redmiles, Ziyun Zhu *(University of Maryland)*, Sean Kross *(University of California, San Diego)*,
  Dhruv Kuchhal *(Maharaja Agrasen Institute of Technology)*,
  Tudor Dumitras, Michelle L. Mazurek *(University of Maryland)*
- **Towards Usable Checksums: Automating the Integrity Verification of Web Downloads for the Masses**..... 1256
  Mauro Cherubini, Alexandre Meylan, Bertil Chapuis *(UNIL-HEC Lausanne)*,
  Mathias Humbert *(Swiss Data Science Center)*, Igor Bilogrevic *(Google Inc.)*,
  Kévin Huguenin *(UNIL-HEC Lausanne)*
- **Investigating System Operators' Perspective on Security Misconfigurations** 1272
  Constanze Dietrich *(Berliner Hochschule für Technik)*, Katharina Krombholz *(CISPA Helmholtz Center (i.G.))*,
  Kevin Borgolte *(Princeton University)*, Tobias Fiebig *(TU Delft)*
- **Peeling the Onion's User Experience Layer: Examining Naturalistic Use of the Tor Browser**..... 1290
  Kevin Gallagher *(New York University)*, Sameer Patil *(Indiana University Bloomington)*,
  Brendan Dolan-Gavitt, Damon McCoy, Nasir Memon *(New York University)*

Session 7A: Forensics

Session Chair: Sadia Afroz *(ICSI, University of California, Berkeley)*

- **PrinTracker: Fingerprinting 3D Printers using Commodity Scanners**..... 1306
  Zhengxiong Li, Aditya Singh Rathore *(SUNY, University at Buffalo)*, Chen Song *(SUNY, University at Buffalo)*,
  Sheng Wei *(Rutgers University)*, Yanzhi Wang *(Northeastern University)*,
  Wenyao Xu *(SUNY, University at Buffalo)*
- **NodeMerge: Template Based Efficient Data Reduction For Big-Data Causality Analysis** 1324
  Yutao Tang *(The College of William and Mary)*, Ding Li, Zhichun Li *(NEC Laboratories America Inc)*,
  Mu Zhang *(Cornell University)*, Kangkook Jee *(NEC Laboratories America Inc)*,
  Xusheng Xiao *(Case Western Reserve University)*, Zhenyu Wu, Junghwan Rhee *(NEC Laboratories America Inc)*,
  Fengyuan Xu *(Nanjing University)*, Qun Li *(The College of William and Mary)*
- **EviHunter: Identifying Digital Evidence in the Permanent Storage of Android Devices via Static Analysis**..... 1338
  Chris Chao-Chun Cheng, Chen Shi, Neil Zhenqiang Gong, Yong Guan *(Iowa State University)*

Session 7B: Formal + LangSec

Session Chair: Andrei Sabelfeld *(Chalmers University of Technology)*

- **When Good Components Go Bad: Formally Secure Compilation Despite Dynamic Compromise** 1351
  Carmine Abate *(Inria Paris & University of Trento)*, Arthur Azevedo de Amorim *(Carnegie Mellon University)*,
  Roberto Blanco *(Inria Paris)*, Ana Nora Evans *(Inria Paris & University of Virginia)*,
  Guglielmo Fachini, Cătălin Hriţcu *(Inria Paris)*, Théo Laurent *(Inria Paris & ENS Paris)*,
  Benjamin C. Pierce *(University of Pennsylvania)*, Marco Stronati *(Inria Paris)*,
  Andrew Tolmach *(Portland State University)*
- **Towards Verified, Constant-time Floating Point Operations**..... 1369
  Marc Andrysco *(University of California, San Diego)*, Andres Nötzli, Fraser Brown *(Stanford University)*,
  Ranjit Jhala, Deian Stefan *(University of California, San Diego)*
- **A Formal Analysis of 5G Authentication** 1383
  David Basin *(ETH Zurich)*, Jannik Dreier *(LORIA, CNRS, Inria, Université de Lorraine)*,
  Lucca Hirschi *(ETH Zurich)*, Saša Radomirović *(University of Dundee)*,
  Ralf Sasse, Vincent Stettler *(ETH Zurich)*

Session 7C: TLS 1

Session Chair: Ehab Al-Shaer *(University of North Carolina)*

- **Pseudo Constant Time Implementations of TLS Are Only Pseudo Secure** 1397
  Eyal Ronen *(Weizmann Institute of Science)*, Kenneth G. Paterson *(Royal Holloway, University of London)*,
  Adi Shamir *(Weizmann Institute of Science)*
- **Partially Specified Channels: The TLS 1.3 Record Layer without Elision** 1415
  Christopher Patton, Thomas Shrimpton *(University of Florida)*
- **The Multi-user Security of GCM, Revisited: Tight Bounds for Nonce Randomization** 1429
  Viet Tung Hoang *(Florida State University)*,
  Stefano Tessaro, Aishwarya Thiruvengadam *(University of California, Santa Barbara)*

Session 7D: BinDef 1

Session Chair: Michael Franz *(University of California, Irvine)*

- **Lord of the x86 Rings: A Portable User Mode Privilege Separation Architecture on x86** 1441
  Hojoon Lee *(CISPA Helmholtz Center i.G.)*,
  Chihyun Song, Brent Byunghoon Kang *(Korea Advanced Institute of Science and Technology)*
- **Milkomeda: Safeguarding the Mobile GPU Interface Using WebGL Security Checks** 1455
  Zhihao Yao, Saeed Mirzamohammadi, Ardalan Amiri Sani *(University of California, Irvine)*,
  Mathias Payer *(EPFL & Purdue University)*
- **Enforcing Unique Code Target Property for Control-Flow Integrity** 1470
  Hong Hu, Chenxiong Qian, Carter Yagemann, Simon Pak Ho Chung *(Georgia Institute of Technology)*,
  William R. Harris *(Georgia Institute of Technology & Galois Inc.)*,
  Taesoo Kim, Wenke Lee *(Georgia Institute of Technology)*

Session 8A: Web 1

Session Chair: Adam Doupé *(Arizona State University)*

- **Predicting Impending Exposure to Malicious Content from User Behavior** 1487
  Mahmood Sharif *(Carnegie Mellon University)*, Jumpei Urakawa *(KDDI Research, Inc.)*,
  Nicolas Christin *(Carnegie Mellon University)*, Ayumu Kubota, Akira Yamada *(KDDI Research, Inc.)*
- **Clock Around the Clock: Time-Based Device Fingerprinting** 1502
  Iskander Sanchez-Rola, Igor Santos *(Deustotech, University of Deusto)*, Davide Balzarotti *(Eurecom)*
- **The Web's Sixth Sense: A Study of Scripts Accessing Smartphone Sensors** 1515
  Anupam Das *(North Carolina State University)*, Gunes Acar *(Princeton University)*,
  Nikita Borisov *(University of Illinois at Urbana-Champaign)*, Amogh Pradeep *(Northeastern University)*

Session 8B: Usable Passwords

Session Chair: Katharina Krombholz *(CISPA Helmholtz Center i.G.)*,

- **Reinforcing System-Assigned Passphrases Through Implicit Learning** 1533
  Zeinab Joudaki, Julie Thorpe, Miguel Vargas Martin *(University of Ontario Institute of Technology)*
- **"What was that site doing with my Facebook password?"**
  Designing Password-Reuse Notifications 1549
  Maximilian Golla *(Ruhr University Bochum)*,
  Miranda Wei, Juliette Hainline, Lydia Filipe *(University of Chicago)*,
  Markus Dürmuth *(Ruhr University Bochum)*, Elissa Redmiles *(University of Maryland)*,
  Blase Ur *(University of Chicago)*
- **On the Accuracy of Password Strength Meters** 1567
  Maximilian Golla, Markus Dürmuth *(Ruhr University Bochum)*

Session 8C: InfoFlows

Session Chair: Yinzhi Cao Cao *(Johns Hopkins University)*

- **HyperFlow: A Processor Architecture for Nonmalleable, Timing-Safe Information Flow Security** 1583
  Andrew Ferraiuolo, Mark Zhao, Andrew C. Myers, G. Edward Suh *(Cornell University)*
- **Runtime Analysis of Whole-System Provenance** 1601
  Thomas Pasquier *(University of Bristol)*, Xueyuan Han *(Harvard University)*, Thomas Moyer, Adam Bates *(University of Illinois at Urbana-Champaign)*, Olivier Hermant *(MINES ParisTech PSL Research University)*, David Eyers *(University of Otago)*, Jean Bacon *(University of Cambridge)*, Margo Seltzer *(University of British Columbia)*
- **Faceted Secure Multi Execution** 1617
  Thomas Schmitz *(University of California, Santa Cruz)*, Maximilian Algehed *(Chalmers University of Technology)*, Cormac Flanagan *(University of California, Santa Cruz)*, Alejandro Russo *(Chalmers University of Technology)*

Session 8D: BinDef 2

Session Chair: Lorenzo Cavallaro *(King's College London)*

- **A Robust and Efficient Defense against Use-after-Free Exploits via Concurrent Pointer Sweeping** 1635
  Daiping Liu *(University of Delaware)*, Mingwei Zhang *(Intel Labs)*, Haining Wang *(University of Delaware)*
- **An Exploratory Analysis of Microcode as a Building Block for System Defenses** 1649
  Benjamin Kollenda, Philipp Koppe, Marc Fyrbiak, Christian Kison, Christof Paar, Thorsten Holz *(Ruhr-Universität Bochum)*
- **Debin: Predicting Debug Information in Stripped Binaries** 1667
  Jingxuan He, Pesho Ivanov, Petar Tsankov *(ETH Zurich)*, Veselin Raychev *(DeepCode AG)*, Martin Vechev *(ETH Zurich)*

Session 9A: Web 2

Session Chair: Ben Stock *(CISPA Helmholtz Center i.G.)*

- **Mystique: Uncovering Information Leakage from Browser Extensions** 1687
  Quan Chen, Alexandros Kapravelos *(North Carolina State University)*
- **How You Get Shot in the Back: A Systematical Study about Cryptojacking in the Real World** 1701
  Geng Hong, Zhemin Yang, Sen Yang, Lei Zhang, Yuhong Nan, Zhibo Zhang, Min Yang, Yuan Zhang *(Fudan University)*, Zhiyun Qian *(University of California, Riverside)*, Haixin Duan *(Tsinghua University)*
- **MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense** 1714
  Radhesh Krishnan Konoth, Emanuele Vineti *(Vrije Universiteit Amsterdam)*, Veelasha Moonsamy *(Utrecht University)*, Martina Lindorfer *(TU Wien)*, Christopher Kruegel *(University of California, Santa Barbara)*, Herbert Bos *(Vrije Universiteit Amsterdam)*, Giovanni Vigna *(University of California, Santa Barbara)*
- **Pride and Prejudice in Progressive Web Apps: Abusing Native App-like Features in Web Applications** 1731
  Jiyeon Lee, Hayeon Kim, Junghwan Park, Insik Shin, Sooel Son *(Korea Advanced Institute of Science and Technology)*

Session 9B: Mobile 2

Session Chair: Gianluca Stringhini *(Boston University)*

- **No Training Hurdles: Fast Training-Agnostic Attacks to Infer Your Typing** 1747
  Song Fang *(University of Oklahoma)*, Ian Markwood, Yao Liu, Shangqing Zhao, Zhuo Lu *(University of South Florida)*, Haojin Zhu *(Shanghai Jiaotong University)*
- **Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion** 1761
  Stefan Savage *(University of California, San Diego)*

- **PatternListener: Cracking Android Pattern Lock Using Acoustic Signals** 1775
  Man Zhou, Qian Wang, Jingxiao Yang *(Wuhan University)*, Qi Li *(Tsinghua University)*,
  Feng Xiao, Zhibo Wang *(Wuhan University)*, Xiaofeng Chen *(Xidian University)*
- **Phishing Attacks on Modern Android** 1788
  Simone Aonzo, Alessio Merlo, Giulio Tavella *(University of Genoa)*, Yanick Fratantonio *(EURECOM)*

Session 9C: Crypto 4

Session Chair: Yan Huang Huang *(Indiana University)*

- **On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees** 1802
  Katriel Cohn-Gordon *(University of Oxford)*, Cas Cremers *(CISPA Helmholtz Center i.G.)*,
  Luke Garratt *(University of Oxford)*, Jon Millican *(Facebook)*, Kevin Milner *(University of Oxford)*
- **Bandwidth-Hard Functions: Reductions and Lower Bounds** 1820
  Jeremiah Blocki *(Purdue University)*, Ling Ren *(Massachusetts Institute of Technology)*,
  Samson Zhou *(Purdue University)*
- **Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody** 1837
  Yehuda Lindell, Ariel Nof *(Bar-Ilan University)*
- **TACHYON: Fast Signatures from Compact Knapsack** 1855
  Rouzbeh Behnia, Muslum Ozgur Ozmen *(Oregon State University)*,
  Attila A. Yavuz *(University of South Florida)*, Mike Rosulek *(Oregon State University)*

Session 9D: VulnDet 1

Session Chair: Tudor Dumitras *(University of Maryland, College Park)*

- **Block Oriented Programming: Automating Data-Only Attacks** 1868
  Kyriakos K. Ispoglou, Bader AlBassam *(Purdue University)*, Trent Jaeger *(Pennsylvania State University)*,
  Mathias Payer *(Purdue University)*
- **Threat Intelligence Computing** 1883
  Xiaokui Shu, Frederico Araujo, Douglas L. Schales, Marc Ph. Stoecklin, Jiyong Jang, Heqing Huang,
  Josyula R. Rao *(IBM Research)*
- **Check It Again: Detecting Lacking-Recheck Bugs in OS Kernels** 1899
  Wenwen Wang, Kangjie Lu, Pen-Chung Yew *(University of Minnesota, Twin Cities)*
- **Revery: From Proof-of-Concept to Exploitable: (One Step towards Automatic Exploit Generation)** 1914
  Yan Wang *(Chinese Academy of Sciences & University of Chinese Academy of Sciences)*,
  Chao Zhang *(Tsinghua University)*,
  Xiaobo Xiang, Zixuan Zhao, Wenjie Li, Xiaorui Gong, Bingchang Liu *(Chinese Academy of Sciences & University of Chinese Academy of Sciences)*, Kaixiang Chen *(Tsinghua University)*,
  Wei Zou *(Chinese Academy of Sciences & University of Chinese Academy of Sciences)*

Session 10A: TOR

Session Chair: Esfandiar Mohammadi *(ETH Zurich)*

- **Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning** 1928
  Payap Sirinam *(Rochester Institute of Technology)*, Mohsen Imani *(University of Texas at Arlington)*,
  Marc Juarez *(imec-COSIC KU Leuven)*, Matthew Wright *(Rochester Institute of Technology)*
- **Privacy-Preserving Dynamic Learning of Tor Network Traffic** 1944
  Rob Jansen, Matthew Traudt *(U.S. Naval Research Laboratory)*, Nicholas Hopper *(University of Minnesota)*
- **DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning** 1962
  Milad Nasr, Alireza Bahramali, Amir Houmansadr *(University of Massachusetts, Amherst)*
- **Measuring Information Leakage in Website Fingerprinting Attacks and Defenses** 1977
  Shuai Li, Huajun Guo, Nicholas Hopper *(University of Minnesota)*

Session 10B: Protocols

Session Chair: Felix Günther *(University of California, San Diego)*

- **DiSE: Distributed Symmetric-key Encryption** 1993
  Shashank Agrawal, Payman Mohassel, Pratyay Mukherjee *(Visa Research)*,
  Peter Rindal *(Oregon State University)*
- **Mitigating Risk while Complying with Data Retention Laws** 2011
  Luis Vargas, Gyan Hazarika *(University of Florida)*, Rachel Culpepper *(University of Richmond)*,
  Kevin R.B. Butler, Thomas Shrimpton *(University of Florida)*, Doug Szajda *(University of Richmond)*,
  Patrick Traynor *(University of Florida)*
- **BEAT: Asynchronous BFT Made Practical** 2028
  Sisi Duan *(University of Maryland, Baltimore County)*,
  Michael K. Reiter *(Univeristy of North Carolina, Chapel Hill)*,
  Haibin Zhang *(University of Maryland, Baltimore County)*
- **PASTA: PASsword-based Threshold Authentication** 2042
  Shashank Agrawal *(Visa Research)*, Peihan Miao *(University of California, Berkeley)*,
  Payman Mohassel, Pratyay Mukherjee *(Visa Research)*

Session 10C: TLS 2

Session Chair: Haining Wang *(University of Delaware)*

- **Domain Validation++ For MitM-Resilient PKI** 2060
  Markus Brandt, Tianxiang Dai, Amit Klein, Haya Shulman,
  Michael Waidner *(Fraunhofer Institute for Secure Information Technology SIT)*
- **Secure Opportunistic Multipath Key Exchange** 2077
  Sergiu Costea *(ETH Zürich)*, Marios O. Choudary, Doru Gucea *(University Politehnica of Bucharest)*,
  Björn Tackmann *(IBM Research – Zürich)*, Costin Raiciu *(University Politehnica of Bucharest)*

Session 10D: VulnDet 2 + Side Channels 2

Session Chair: Alexandros Kapravelos *(NC State University)*

- **Hawkeye: Towards a Desired Directed Grey-box Fuzzer** 2095
  Hongxu Chen *(Nanyang Technological University)*, Yinxing Xue *(University of Science and Technology of China)*,
  Yuekang Li *(Nanyang Technological University)*, Bihuan Chen *(Fudan University)*,
  Xiaofei Xie, Xiuheng Wu, Yang Liu *(Nanyang Technological University)*
- **ret2spec: Speculative Execution Using Return Stack Buffers** 2109
  Giorgi Maisuradze, Christian Rossow *(CISPA, Saarland University)*
- **Evaluating Fuzz Testing** 2123
  George Klees, Andrew Ruef, Benji Cooper *(University of Maryland)*, Shiyi Wei *(University of Texas at Dallas)*,
  Michael Hicks *(University of Maryland)*
- **Rendered Insecure: GPU Side Channel Attacks are Practical** 2139
  Hoda Naghibijouybari, Ajaya Neupane, Zhiyun Qian, Nael Abu-Ghazaleh *(University of California, Riverside)*

Tutorials

- **Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning: Half-day Tutorial** 2154
  Battista Biggio, Fabio Roli *(University of Cagliari)*
- **Secure Multi-Party Computation** 2157
  Fattaneh Bayatbabolghani *(University of California, Berkeley)*,
  Marina Blanton *(University at Buffalo, The State University of New York)*
- **Building Applications with Homomorphic Encryption** 2160
  Roger A. Hallman *(SPAWAR Systems Center Pacific & Dartmouth College)*, Kim Laine *(Microsoft Research)*,
  Wei Dai *(Worcester Polytechnic Institute)*, Nicolas Gama *(Inpher, Inc.)*, Alex J. Malozemoff *(Galois, Inc)*,
  Yuriy Polyakov *(NJIT Cybersecurity Research Center)*, Sergiu Carpov *(CEA, LIST)*
- **Game Theory Meets Network Security: A Tutorial** 2163
  Quanyan Zhu *(New York University)*, Stefan Rass *(Universitaet Klagenfurt)*

Workshop Summaries

- **11th International Workshop on Artificial Intelligence and Security (AISec 2018)** 2166
  Sadia Afroz *(ICSI, University of California, Berkeley)*, Battista Biggio *(University of Cagliari)*,
  Yuval Elovici *(Ben-Gurion University of the Negev)*, David Freeman *(Facebook, Inc.)*,
  Asaf Shabtai *(Ben-Gurion University of the Negev)*
- **ASHES 2018 — Workshop on Attacks and Solutions in Hardware Security** 2168
  Chip Hong Chang *(NTU Singapore)*, Jorge Guajardo *(Robert Bosch LLC – RTC)*,
  Daniel Holcomb *(UMass Amherst)*, Francesco Regazzoni *(ALaRI - USI)*,
  Ulrich Rührmair *(Ruhr-University Bochum)*
- **CPS-SPC 2018: Fourth Workshop on Cyber-Physical Systems Security and PrivaCy** 2171
  Awais Rashid *(University of Bristol)*, Nils Ole Tippenhauer *(CISPA Helmholtz-Zentrum i.G.)*
- **2nd International Workshop on Multimedia Privacy and Security** 2173
  Roger A. Hallman *(SPAWAR Systems Center Pacific & Dartmouth College)*, Shujun Li *(University of Kent)*,
  Victor Chang *(Xi'an Jiaotong-Liverpool University)*
- **MTD 2018: 5th ACM Workshop on Moving Target Defense (MTD)** 2175
  Massimiliano Albanese *(George Mason University)*, Dijiang Huang *(Arizona State University)*
- **SecArch'18: 1st Workshop of Security-Oriented Designs of Computer Architectures and Processors** 2177
  Dan Meng *(Institute of Information Engineering, Chinese Academy of Sciences)*
- **PLAS 2018 - ACM SIGSAC Workshop on Programming Languages and Analysis for Security** 2178
  Mário S. Alvim *(UFMG)*, Stéphanie Delaune *(Univ Rennes, CNRS, IRISA)*
- **SysTEX'18: 2018 Workshop on System Software for Trusted Execution** 2180
  Baris Kasikci *(University of Michigan)*, Mark Silberstein *(Technion)*
- **17th Workshop on Privacy in the Electronic Society (WPES 2018)** 2181
  Aaron Johnson *(U.S. Naval Research Laboratory)*, Ryan Henry *(University of Calgary)*
- **WAHC'18: 6thWorkshop on Encrypted Computing and Applied Homomorphic Cryptography** 2183
  Michael Brenner *(Leibniz Universität Hannover)*, Kurt Rohloff *(New Jersey Institute of Technology)*
- **FEAST'18 – 2018 Workshop on Forming an Ecosystem Around Software Transformation** ... 2185
  Yan Shoshitaishvili *(Arizona State University)*, Mayur Naik *(University of Pennsylvania)*

Panel

- **A Discussion on Security Education in Academia** 2187
  Kevin Butler *(University of Florida)*, Robert K. Cunningham *(Carnegie Mellon University)*,
  Paul C. van Oorschot *(Carleton University)*, Reihaneh Safavi-Naini *(University of Calgary)*,
  Ashraf Matrawy *(Carleton University)*, Jeremy Clark *(Concordia University)*

Demonstrations

- **DEMO: An Effective Android Code Coverage Tool** 2189
  Aleksandr Pilgun, Olga Gadyatskaya, Stanislav Dashevskyi *(University of Luxembourg)*,
  Yury Zhauniarovich *(Qatar Computing Research Institute)*, Artsiom Kushniarou *(University of Luxembourg)*
- **DEMO: PrivacyBuDe: Privacy Buckets Demo Tight Differential Privacy Guarantees made Simple** 2192
  David Sommer *(ETH Zurich)*, Sebastian Meiser *(University College London)*, Esfandiar Mohammadi *(ETH Zurich)*

Poster Presentations

- **POSTER: A Re-evaluation of Intrusion Detection Accuracy: an Alternative Evaluation Strategy** 2195
  Said Al-Riyami, Frans Coenen, Alexei Lisitsa *(Liverpool University)*
- **POSTER: How to Choose Suitable Secure Multiparty Computation Using Generalized SPDZ** 2198
  Toshinori Araki *(NEC)*, Assi Barak *(Bar-Ilan University)*, Jun Furukawa *(NEC Israel Research Center)*, Marcel Keller *(Data61)*, Kazuma Ohara, Hikaru Tsuchida *(NEC)*
- **POSTER: Hardware Acceleration of Searchable Encryption** 2201
  Arnab Bag, Sikhar Patranabis *(Indian Institute of Technology Kharagpur)*, L. Tribhuvan *(BMS College of Engineering)*, Debdeep Mukhopadhyay *(Indian Institute of Technology Kharagpur)*
- **POSTER: Practical Fault Attack on Deep Neural Networks** 2204
  Jakub Breier, Xiaolu Hou, Dirmanto Jap *(Nanyang Technological University)*, Lei Ma *(Harbin Institute of Technology)*, Shivam Bhasin, Yang Liu *(Nanyang Technological University)*
- **POSTER: FlowNotation: An Annotation System for Statically Enforcing Information Flow Policies in C** 2207
  Darion Cassel *(Carnegie Mellon University)*, Yan Huang *(Indiana University)*, Limin Jia *(Carnegie Mellon University)*
- **POSTER: Cracking the TSCH Channel Hopping in IEEE 802.15.4e** 2210
  Xia Cheng, Mo Sha *(State University of New York at Binghamton)*
- **Poster: Off-Path Attacks Against PKI** 2213
  Tianxiang Dai *(Fraunhofer SIT)*, Haya Shulman, Michael Waidner *(Fraunhofer SIT & TU Darmstadt)*
- **POSTER: The Influence of Code Coverage Metrics on Automated Testing Efficiency in Android** 2216
  Stanislav Dashevskyi, Olga Gadyatskaya, Aleksandr Pilgun *(University of Luxembourg)*, Yury Zhauniarovich *(Qatar Computing Research Institute, HBKU)*
- **POSTER: Toward Trustworthy Deep Learning in Security** 2219
  Wooyoung Go, Daewoo Lee *(National Security Research Institute)*
- **POSTER: Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams** 2222
  Ryo Iijima, Shota Minami, Zhou Yunao *(Waseda University)*, Tatsuya Takehisa, Takeshi Takahashi *(National Institute of Information and Communications Technology)*, Yasuhiro Oikawa, Tatsuya Mori *(Waseda Univerisity)*
- **POSTER: Adversarial Traces for Website Fingerprinting Defense** 2225
  Mohsen Imani *(University of Texas at Arlington)*, Mohammad Saidur Rahman, Matthew Wright *(Rochester Institute of Technology)*
- **POSTER: Towards Understanding the Dynamics of Adversarial Attacks** 2228
  Yujie Ji, Ting Wang *(Lehigh University)*
- **POSTER: Circular AON: A Very Fast Scheme to Protect Encrypted Data Against Key Exposure** 2231
  Katarzyna Kapusta, Gerard Memmi *(Telecom ParisTech)*
- **POSTER: CipherLocker: Encrypted File Sharing with Ranked Search https://cipherlocker.com** 2234
  Jan Kasiak, Bogdan Carbunar, Jake Christensen, Maria Lyukova, Sumeet Bajaj, Mike Boruta, Radu Sion *(Private Machines Inc.)*, Viorel Popescu, Alex Sorodoc, Gabriel Stan *(Privacy Systems SRL)*
- **POSTER: A Guided Approach to Behavioral Authentication** 2237
  Yeeun Ku, Leo Hyun Park, Sooyeon Shin, Taekyoung Kwon *(Yonsei University)*
- **POSTER: Cryptographically Secure Detection of Injection Attacks** 2240
  Yun Lu, Konstantinos Mitropoulos *(University of Edinburgh)*, Rafail Ostrovsky *(University of California, Los Angeles)*, Avraham Weinstock *(Rensselaer Polytechnic Institute)*, Vassilis Zikas *(University of Edinburgh)*
- **POSTER: Can Browser Add-Ons Protect Your Children from Online Tracking?** 2243
  Zachary Matthews, Natalija Vlajic *(York University)*

- **POSTER: Spartan Networks: Self-Feature-Squeezing Networks for Increased Robustness in Adversarial Settings** 2246
  François Menet, Paul Berthier, Michel Gagnon, José M. Fernandez *(Polytechnique Montréal)*
- **Poster: Knowledge Seeking on The Shadow Brokers** 2249
  Seung Ho Na, Kwanwoo Kim, Seungwon Shin *(Korea Advanced Institute of Science and Technology)*
- **POSTER: Assessing Non-Visual SSL Certificates with Desktop and Mobile Screen Readers**. 2252
  Daniela Napoli, Sonia Chiasson *(Carleton University)*
- **POSTER: The House That Knows You: User Authentication Based on IoT Data** 2255
  Talha Ongun, Alina Oprea, Cristina Nita-Rotaru *(Northeastern University)*,
  Mihai Christodorescu, Negin Salajegheh *(Visa Research)*
- **POSTER: A Storage-level Detection Mechanism against Crypto–Ransomware** 2258
  Joon-Young Paik *(Tianjin Polytechnic University)*, Joong-Hyun Choi *(Chungnam National University)*,
  Rize Jin, Jianming Wang *(Tianjin Polytechnic University)*, Eun-Sun Cho *(Chungnam National University)*
- **POSTER: The Price of Privacy in Collaborative Learning** 2261
  Balázs Pejó *(University of Luxembourg)*, Qiang Tang *(Luxembourg Institute of Science and Technology)*,
  Gergely Biczók *(Budapest University of Technology and Economics)*
- **POSTER: Enabling Fair ML Evaluations for Security** 2264
  Feargus Pendlebury, Fabio Pierazzi, Roberto Jordaney *(Royal Holloway, University of London & King's College London)*,
  Johannes Kinder *(Royal Holloway, University of London)*, Lorenzo Cavallaro *(King's College London)*
- **POSTER: Towards Architecture and OS-Independent Malware Detection via Memory Forensics** 2267
  Rachel Petrik *(University of Kentucky)*, Berat Arik *(University of Tennessee, Knoxville)*,
  Jared M. Smith *(Oak Ridge National Laboratory & University of Tennessee, Knoxville)*
- **POSTER: Equitable Security: Optimizing Distribution of Nudges and Resources** 2270
  Elissa M. Redmiles, John P. Dickerson *(University of Maryland)*,
  Krishna P. Gummadi *(Max Planck Institute for Software Systems)*, Michelle L. Mazurek *(University of Maryland)*
- **POSTER: Public Order Preserving Cipher Generation Scheme for Distributed Computing**. 2273
  Amrita Roy Chowdhury, Parameswaran Ramanathan *(University of Wisconsin-Madison)*
- **POSTER: AST-Based Deep Learning for Detecting Malicious PowerShell** 2276
  Gili Rusak *(Stanford University)*, Abdullah Al-Dujaili, Una-May O'Reilly *(Massachusetts Institute of Technology)*
- **Poster: Aggregated Machine Learning on Indicators of Compromise in Android Devices** ... 2279
  John M. San Miguel, Megan E. M. Kline *(SPAWAR Systems Center Pacific)*,
  Roger A. Hallman *(SPAWAR Systems Center Pacific & Dartmouth College)*,
  Scott M. Slayback *(SPAWAR Systems Center Pacific)*, Alexis Rogers, Stefanie S. F. Chang *(Naval Postgraduate School)*
- **POSTER: End-to-End Secure Mobile Group Messaging with Conversation Integrity and Minimal Metadata Leakage** 2282
  Michael Schliep, Nicholas Hopper *(University of Minnesota)*
- **POSTER: Not All Pixels are Born Equal: An Analysis of Evasion Attacks under Locality Constraints** 2285
  Vikash Sehwag, Chawin Sitawarin, Arjun Nitin Bhagoji, Arsalan Mosenia, Mung Chiang, Prateek Mittal *(Princeton University)*
- **POSTER: Post-quantum Security using Channel Noise** 2288
  Setareh Sharifian, Reihaneh Safavi-Naini *(University of Calgary)*, Fuchun Lin *(Nanyang Technological University)*
- **Poster: Image Disguising for Privacy-preserving Deep Learning** 2291
  Sagar Sharma, Keke Chen *(Wright State University)*
- **Poster: Privacy-Preserving Boosting with Random Linear Classifiers** 2294
  Sagar Sharma, Keke Chen *(Wright State University)*
- **POSTER: Restricting Control Flow During Speculative Execution** 2297
  Zhuojia Shen, Jie Zhou, Divya Ojha, John Criswell *(University of Rochester)*

- **POSTER: Removing the Bottleneck for Practical 2PC** 2300
  Kris Shrishak *(TU Darmstadt)*, Haya Shulman, Michael Waidner *(Fraunhofer SIT & TU Darmstadt)*
- **POSTER: Cashing in on the File-System Cache** 2303
  Trishita Tiwari, Ari Trachtenberg *(Boston University)*
- **POSTER: Facilitating Privacy-preserving Recommendation-as-a-Service with Machine Learning** 2306
  Jun Wang, Afonso Arriaga *(University of Luxembourg)*, Qiang Tang *(Luxembourg Institute of Science and Technology)*, Peter Y.A. Ryan *(University of Luxembourg)*
- **POSTER: Medical Devices are at Risk: Information Security on Diagnostic Imaging System** 2309
  Zhiqiang Wang *(Beijing Electronic Science and Technology Institute & Anhui Province Key Laboratory of Industry Safety and Emergency Technology)*, Pingchuan Ma, Yaping Chi, Jianyi Zhang *(Beijing Electronic Science and Technology Institute)*
- **POSTER: Practical and Privacy-Aware Truth Discovery in Mobile Crowd Sensing Systems** 2312
  Guowen Xu, Hongwei Li *(University of Electronic Science and Technology of China)*, Rongxing Lu *(University of New Brunswick)*
- **POSTER: MORPH: Enhancing System Security through Interactive Customization of Application and Communication Protocol Features** 2315
  Hongfa Xue, Yurong Chen, Guru Venkataramani, Tian Lan *(George Washington University)*, Guang Jin, Jason Li *(Intelligent Automation Inc.)*
- **POSTER: A Bitstream Reverse Engineering Tool for FPGA Hardware Trojan Detection** 2318
  Junghwan Yoon, Yezee Seo, Jaedong Jang, Mingi Cho *(Yonsei University)*, JinGoog Kim, HyeonSook Kim *(Agency of Defense Department)*, Taekyoung Kwon *(Yonsei University)*
- **POSTER: A Markov Decision Process to Determine Optimal Policies in Moving Target** 2321
  Jianjun Zheng, Akbar Siami Namin *(Texas Tech University)*
- **POSTER: Adversarial Product Review Generation with Word Replacements** 2324
  Yimin Zhu, Simon S. Woo *(The State University of New York, Korea)*

Author Index 2327

ACM CCS 2018 Conference Organization

General Chairs: David Lie *(University of Toronto)*
Mohammad Mannan *(Concordia University)*

Program Chairs: Michael Backes *(CISPA Helmholtz Center i.G.)*
XiaoFeng Wang *(Indiana University)*

Workshop Chairs: Rei Safavi-Naini *(University of Calgary)*
Ali Miri *(Ryerson University)*

Tutorial Chairs: Douglas Stebila *(University of Waterloo)*
Brent Byunghoon Kang *(Korea Advanced Institute of Science and Technology)*

Poster/Demo Chairs: Elizabeth Stobert *(Concordia University)*
David Barrera *(Polytechnique Montreal)*

Treasurers: Sergey Gorbunov *(University of Waterloo)*
Miguel Vargas Martin *(University of Ontario Institute of Technology)*

Web Chairs: Anil Somayaji *(Carleton University)*
Julie Thorpe *(University of Ontario Institute of Technology)*

Panels Chairs: Ashraf Matrawy *(Carleton University)*
Jeremy Clark *(Concordia University)*

Registration Chair: Glenn Wurster *(BlackBerry)*

Student Travel Grant Chairs: Aanjhan Ranganathan *(Northeastern University)*
Kari Kostiainen *(ETH Zurich)*
Joel Reardon *(University of Calgary)*
Hassan Takabi *(University of North Texas)*

Social Media Chairs: Long Lu *(Northeastern University)*
Aleksander Essex *(Western University)*

Proceedings Chairs: Ryan Henry *(University of Calgary)*
Aniket Kate *(Purdue University)*

Local Arrangements Chair: Ivan Pustogarov *(University of Toronto)*
Zhen Huang *(PennState)*

Sponsor/Industry Outreach Chairs: Andrew Paverd *(Aalto University)*
Tao Wan *(CableLabs)*

Volunteer Coordinator/Chair: Amirali Abari *(University of Ontario Institute of Technology)*

Steering Committee Chair: Somesh Jha *(University of Wisconsin-Madison)*

Publicity Chairs: Natalija Vlajic *(York University)*
Vijay Ganesh *(University of Waterloo)*
Manuel Egele *(Boston University)*
Aravind Prakash *(Binghamton University)*

Steering Committee: Rebecca Wright *(Rutgers University)*
Carl Landwehr *(George Washington University)*
Giovanni Vigna *(University of California-Santa Barbara)*
George Danezis *(University College London)*
Trent Jaeger *(Pennsylvania State University)*
Stefan Savage *(University of California-San Diego)*
David Basin *(ETH Zurich)*

Program Committee Area Chairs: Haibo Chen *(Shanghai Jiao Tong University)*
Emiliano de Cristofaro *(University College London)*
Manuel Egele *(Boston University)*
Guofei Gu *(Texas A&M University)*
Jonathan Katz *(University of Maryland)*
Andrei Sabelfeld *(Chalmers)*

Program Committee: Alessandro Acquisti *(Carnegie Mellon University)*
Sadia Afroz *(ICSI)*
Gail-Joon Ahn *(Arizona State University and SAMSUNG Research)*
Devdatta Akhawe *(Dropbox)*
Ehab Al-Shaer *(UNC Charlotte)*
Sumayah Alrwais *(King Saud University)*
Dennis Andriesse *(VU Amsterdam)*
Giuseppe Ateniese *(Stevens Institute of Technology)*
Erman Ayday *(Case Western Reserve University)*
Foteini Baldimtsi *(George Mason University)*
Shehar Bano *(UCL)*
Gilles Barthe *(IMDEA)*
Lujo Bauer *(Carnegie Mellon University)*
Mihir Bellare *(University of California, San Diego)*
Fabrice Benhamouda *(Columbia University)*
Karthik Bhargavan *(INRIA)*
Battista Biggio *(University of Cagliari)*
Alex Biryukov *(University of Luxembourg)*
Nikita Borisov *(UIUC)*
Sven Bugiel *(CISPA Helmholtz Center i.G.)*
Yinzhi Cao *(Lehigh University)*
Srdjan Capkun *(ETH Zurich)*
Lorenzo Cavallaro *(Royal Holloway)*
Kai Chen *(Institute of Information Engineering, Chinese Academy of Sciences)*

Program Committee (continued): Shuo Chen *(Microsoft Research)*
Yan Chen *(Northwestern)*
Hao Chen *(University of California, Davis)*
Omar Chowdhury *(University of Iowa)*
Nicolas Christin *(Carnegie Mellon University)*
Henry Corrigan-Gibbs *(Stanford)*
Veronique Cortier *(LORIA)*
Cas Cremers *(Oxford University)*
Weidong Cui *(Microsoft Research)*
Lucas Davi *(University of Duisburg-Essen)*
Wenrui Diao *(Jinan University)*
Adam Doupé *(Arizona State University)*
Haixin Duan *(Tsinghua)*
Tudor Dumitras *(University of Maryland)*
Zakir Durumeric *(Stanford)*
Serge Egelman *(University of California, Berkeley)*
Roya Ensafi *(University of Michigan)*
Dave Evans *(University of Virginia)*
Sascha Fahl *(Ruhr-University Bochum)*
Dario Fiore *(IMDEA)*
Marc Fischlin *(TU Darmstadt)*
Michael Franz *(University of California, Irvine)*
Debin Gao *(Singapore Management University)*
Christina Garman *(Purdue University)*
Xinyang Ge *(MSR)*
Rosario Gennaro *(City College of New York)*
Arthur Gervais *(Imperial College London)*
Irene Giacomelli *(UW Madison)*
Virgil Gligor *(Carnegie Mellon University)*
Neil Gong *(Iowa State University)*
Daniel Gruss *(TU Graz)*
Dawu Gu *(Shanghai JiaoTong University)*
Weili Han *(Fudan)*
Ryan Henry *(Indiana University)*
Nicholas Hopper *(University of Minnesota)*
Catalin Hritcu *(Inria Paris)*
Yan Huang *(Indiana University)*
Mathias Humbert *(Swiss Data Science Center)*
Tibor Jager *(University of Paderborn)*
L Jean Camp *(Indiana University)*
Shouling Ji *(Zhejing University)*
Yier Jin *(University of Florida)*
Byunghoon Kang *(KAIST)*

Program Committee (continued): Chris Kanich *(UIC)*
Apu Kapadia *(Indiana University)*
Alexandros Kapravelos *(NC State University)*
Aniket Kate *(Purdue)*
Taesoo Kim *(Georgia Tech)*
Yongdae Kim *(KAIST)*
Engin Kirda *(Northeastern University)*
Boris Köpf *(IMDEA Software Institute)*
Katharina Krombholz *(SBA Research)*
Kehuan Zhang *(The Chinese University of Hong Kong)*
Fengwei Zhang *(Wayne State University)*
Zhe Zhou *(Fudan)*
Ralf Kuesters *(University of Stuttgart)*
Wenke Lee *(Georgia Tech)*
Ruby Lee *(Princeton)*
Byoungyoung Lee *(Purdue)*
Anja Lehmann *(IBM Research)*
Zhenkai Liang *(National University of Singapore)*
Xiaojing Liao *(William and Mary)*
Ninghui Li *(Purdue)*
Zhou Li *(RSA Research)*
Yingjiu Li *(Singapore Management University)*
Jingqiang Lin *(Institute of Info. Engineering, Chinese Academy of Sciences))*
Zhiqiang Lin *(Ohio State University)*
Yang Liu *(Nanyang Technical University)*
Peng Liu *(PennState)*
Long Lu *(Northeastern University)*
Songwu Lu *(University of California, Los Angeles)*
Kangjie Lu *(University of Minnesota)*
Matteo Maffei *(TU Vienna)*
Jean-Yves Marion *(LORIA)*
Michelle Mazurek *(University of Maryland)*
Patrick McDaniel *(PennState)*
Ian Miers *(Cornell Tech)*
Esfandiar Mohammadi *(ETH Zurich)*
Tal Moran *(IDC Herzliya)*
Adwait Nadkarni *(William & Mary)*
Muhammad Naveed *(USC)*
Stefan Nuernberger *(CISPA Helmholtz Center i.G.)*
Olya Ohrimenko *(Microsoft Research)*
Nils Ole Tippenhauer *(Singapore University of Technology and Design)*
Nicolas Papernot *(PennState)*
Kenny Paterson *(Royal Holloway)*

Program Committee (continued):

Mathias Payer *(Purdue)*
Giancarlo Pellegrino *(Stanford University)*
Frank Piessens *(KU Leuven)*
Zhiyun Qian *(University of California, Riverside)*
Brad Reaves *(NC State University)*
William Roberson *(Northeastern)*
Ulrich Rührmair *(Ruhr-University Bochum)*
Nitesh Saxena *(University of Alabama at Birmingham)*
Joshua Schiffman *(HP Labs, HP Inc.)*
Felix Schuster *(Microsoft Research)*
Srinath Setty *(Microsoft Research)*
Matthew Smith *(University of Bonn & Fraunhofer FKIE)*
Chenyu Song *(University of California, Riverside)*
Ben Stock *(CISPA Helmholtz Center i.G.)*
Gianluca Stringhini *(University College London)*
Yuqiong Sun *(Symantec Research)*
Bjoern Tackmann *(IBM Research)*
Abhradeep Thakurta *(UC Santa Cruz)*
Yuan Tian *(University of Virginia)*
Mohit Tiwari *(UT Austin)*
Patrick Traynor *(University of Florida)*
Carmela Troncoso *(EPFL)*
Gene Tsudik *(University of California, Irvine)*
Blase Ur *(University of Chicago)*
Venkat Venkatakrishnan *(University of Illinois)*
Hayawardh Vijayakumar *(Samsung Research America)*
Haining Wang *(University of Delaware)*
Bogdan Warinschi *(Bristol)*
Dinghao Wu *(PennState)*
Tao Xie *(UIUC)*
Luyi Xing *(Indiana University Bloomington)*
Xinyu Xing *(PennState)*
Meng Xu *(Georgia Tech)*
Wenyuan Xu *(Zhejing University)*
Min Yang *(Fudan)*
Daphne Yao *(Virginia Tech)*
Heng Yin *(University of California, Riverside)*
Ting Yu *(Qatar Computing Research Institute)*
Yinqian Zhang *(Ohio State University)*
Danfeng Zhang *(PennState)*
Xiangyu Zhang *(Purdue)*

Additional Reviewers: Davide Maiorca
Tousif Ahmed
Zhenhua Chen
Swarup Chandra
Shirin Nilizadeh
Donald S. Williamson
Anupam Das
Adam Aviv
Stelvio Cimato
Stijn Volckaert
Yeoul Na
Michael Schwarz
Moritz Lipp
Elena Pagnin
Ethan Gertler
Panagiotis Chatzigiannis
Antonio Faonio
Sebastian Faust
Sophia Yakoubov
Marios Isaakidis
Varun Madathil
Wing Lam
Xusheng Li
Juanru Li
Xueqing Liu
Xusheng Xiao
Siwakorn Srisakaokul
Wei Yang
Zexuan Zhong
Giuseppe Persiano
Miguel Ambrona
Arwa Alrawais
Ruiyu Zhu
Wenbo Guo
Vincent Laporte
Philipp Rümmer
Henrik Sandberg
Simon Chung
Evan Downing
Joey Allen
Erkam Uzun
Carter Yagemann
Matthew Landen
Mohamed Y. Nabeel
Ioannis Demertzis
David Sommer
Lara Schmid
Briland Hitaj
Olivier Sanders
Joseph Lallemand
Jannik Dreier
Ananth Raghunathan
Yannick Seurin
Mainuddin Jonas
Vishal Karande
Weilin Xu
Yue Duan
Lian Gao
Jie Hu
Brian Testa
Jinghan Wang
Wei Song
Yufei Jiang
Francisco Rocha
Huasong Shan
Xiao Liu
Rupesh Prajapati
Wubing Wang
Pei Wang
Dongpeng Xu
Haohuang Wen
Shuai Wang
Fabio Pierazzi
Roberto Jordaney
Feargus Pendlebury
Xutong Chen
Xue Leng
David Wu
Florian Tramer
Saba Eskandarian
Dmitry Kogan
Ilya Mironov
Yinbo Yu
Maggie Oates
Raphael Bost
Hana Habib

Additional Reviewers (continued):

William Melicher
Chunlin Xiong
Qingchuan Zhao
Chaoshhun Zuo
Xing Li
Xuechao Du
Zhenyuan Li
Kaiyu Hou
Boyuan He
Mathy Vanhoef
Jan Tobias Muehlberg
Raoul Strackx
Jo Van Bulck
Esha Ghosh
Matthias Fassl
Katharina Pfeffer
Matthias Gusenbauer
Rebekah Overdorf
Simon Oya
Bogdan Kulynych
Natalia Kulatova
Arthur Azevedo de Amorim
Benjamin Lipp
Jean Yang
Patrick Derbez
Borja Balle Pigem
Prasad Naldurg
Daniel Feher
Sergei Tikhomirov
Qingju Wang
Aleksei Udovenko
Dag Arne Osvik
Jacqueline Brendel
Patrick Harasser
Jean Paul Degabriele
Christian Janson
Sogol Mazaheri
Jiongyi Chen
Shuaike Dong
Fenghao Xu
Di Tang
Menghan Sun
Shuai Hao
Xing Gao
Daiping Liu
Ludovic Perret
Geoffroy Couteau
Tzipora Halevi
Marie Walter
Peter Honeyman
Matthew Bernhard
Carsten Baum
Patrick Hough
Jonathan Bootle
Robert Brotzman-Smith
Peixuan Li
Adrian Shaw
Remy Husson
Thalia Laing
Marius Steffens
Aurore Fass
Pepe Vila
Michael Nielsen
Sudarsun Kannan
Gabriele Spini
Andrea Cerulli
Mario Di Raimondo
Ruxandra Olimid
Marcel Keller
Maciej Obremski
Dragos Rotaru
Satrajit Ghosh
Amrita Roy Chowdhury
Moosa Yahyazadeh
Yigitcan Kaya
Virinchi Srinivas
Doowon Kim
BumJun Kwon
Sanghyun Hong
Ziyun Zhu
Xiaoyang Cheng
Yan Lin
Xiaoxiao Tang
Pedro Moreno-Sanchez
Baojun Liu
Jianjun Chen

Additional Reviewers (continued):

Xiaofeng Zheng
Hao Yang
Yiming Zhang
Hao Yang
Binanda Sengupta
Hongjun Wu
Bing Chang
Ke Xu
Yangguang Tian
Daibin Wang
Ling Jin
Tiantian Zhu
Yangfan Zhou
Yu Kang
Yuedong Xu
Sherman Chow
Sebastian Surminski
Michael Rodler
Ferdinand Brasser
Luis Garcia
Kai Gellert
David Niehues
Pascal Bemmann
David Derler
Rafael Kurek
Paul Rösler
Friedrich Wiemer
Jinsoo Jang
Hojoon Lee
Daehee Jang
Jiseong Noh
Changho Choi
Jonghwan Kim
Jaehyuck Lee
Sungman Lee
Marshall Ball
Hong Hu
Jian Mao
Yanhao Wang
Zheng Leong Chua
Ziqi Yang
Ben Niu
Jonathan Lee

ACM CCS 2018 Sponsor & Patrons

Sponsor

Platinum Patron

Gold Patrons

Silver Patrons