November 11-15, 2019
London, United Kingdom

Association for
Computing Machinery

Advancing Computing as a Science & Profession

CCS'19

Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security

Sponsored by:

ACM SIGSAC

General Chairs:

Lorenzo Cavallaro (King's College London, UK)
Johannes Kinder (Bundeswehr University Munich, Germany)

Program Chairs:

XiaoFeng Wang (Indiana University, USA)
Jonathan Katz (George Mason University, USA)

Association for
Computing Machinery

Advancing Computing as a Science & Profession

The Association for Computing Machinery
1601 Broadway, 10th Floor
New York, NY 10019-7434

Copyright © 2019 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.

ISBN: 978-1-4503-6747-9

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

It is with great pleasure that we welcome you all to the 2019 edition of the ACM Conference on Computer and Communications Security (CCS). CCS is the flagship annual conference of ACM's Special Interest Group on Security, Audit and Control (SIGSAC), which has been bringing together world-leading academic researchers and practitioners interested in computer security at large since 1993. As in previous years, CCS 2019 features an outstanding program of thought-provoking and cutting-edge research papers. In addition, a record number of 18 workshops provide a forum for in-depth discussions of established and emerging research topics alike.

London is one of the most vibrant metropolises in the world and has something to offer for everyone, whether you are a first-time visitor or a long-time resident. Did you know that London boasts four World Heritage Sites? The Tower of London; Kew Gardens; Westminster Abbey and its surroundings; and the historic settlement in Greenwich. But there is much more! A wide range of world-class museums, most of which are free to visit, restaurants catering to any palate, with cuisines from every corner of the planet, countless cozy pubs and trendy bars, theatres, musicals, and over 20 major universities and about 400,000 students.

CCS would not be possible without you, the community, and the many volunteers working tirelessly to make an event of this scale happen. We would like to thank the authors, who submitted their best work to this conference; the program chairs and the program committee for putting together an excellent program; the steering committee and SIGSAC for providing behind-the-scenes support; and of course the organizing committee who spent many hours on administrative and organizational tasks. Finally, we thank the numerous sponsors of the conference for their generous support.

As a city that prides itself in its diversity and international atmosphere, London is a fitting place to host a conference dedicated to sharing ideas about security and privacy in a diverse and international community. Especially in times of political uncertainty, we should celebrate the free exchange of ideas.

Welcome to London, we hope you will enjoy your stay!

Lorenzo Cavallaro
ACM CCS 2019 General Co-chair
King's College London

Johannes Kinder
ACM CCS 2019 General Co-chair
Bundeswehr University Munich

Program Chairs' Welcome

For the first time in its long history as the ACM's flagship security and privacy conference, CCS this year experimented with a new multi-cycle review model. The model is characterized by two normal submission deadlines (February and May), each with a 2.5-month review cycle. At the end of each cycle, each submitted paper is given a decision of accept, conditional accept (shepherd), reject, or revise. A revised paper can be resubmitted, after the authors have a full month to address reviewers' comments. This new model is designed to facilitate author-reviewer interactions and enhance paper quality.

The February cycle received 220 submissions, with 14 accepted or shepherded and 22 receiving the revision decision. 736 papers were submitted to the May cycle, where 91 papers were accepted or conditionally accepted, and an additional 54 papers were selected to be revised. Altogether, 149 out of 934 submissions were accepted into this year's program, for an acceptance rate of 16.0%. All submissions were reviewed by a program committee of 177 security and privacy experts from around the world, with the vast majority of accepted papers having 4-5 reviews.

The accepted papers cover a wide range of security and privacy topics, from applied cryptography to machine learning to IoT security to hardware security. This diversity showcases the breadth of applied security and privacy research going on nowadays.

To help manage the large number of submissions, 8 area chairs were invited to assist the 2 PC chairs in handling the submissions in their individual areas, guiding the paper-discussion process and helping the chairs select papers. The area chairs were also involved in award paper selection. We thank the area chairs and all other PC members and external reviewers for their contributions to the conference and for their professionalism. We are also grateful to the General Chairs, Lorenzo Cavallaro and Johannes Kinder, for taking care of other organizational issues; to the Proceedings Chairs, Brendan Dolan-Gavitt and Gianluca Stringhini, for working with the publisher to produce the proceedings; and to Xueqiang Wang for managing the submission and paper assignment systems. We also thank all the authors for submitting to CCS.

We hope you enjoy the conference!

XiaoFeng Wang Indiana University at Bloomington	**Jonathan Katz** George Mason University

Table of Contents

CCS 2019 Conference Organization xxii

ACM CCS 2019 Sponsors & Supporters xxix

Session 1A: Attack I

- ***1 Trillion Dollar Refund*** **– How To Spoof PDF Signatures** 1
  Vladislav Mladenov, Christian Mainka *(Ruhr University Bochum)*,
  Karsten Meyer zu Selhausen *(Hackmanit GmbH)*,
  Martin Grothe, Jörg Schwenk *(Ruhr University Bochum)*
- **Practical Decryption exFiltration: Breaking PDF Encryption** 15
  Jens Müller *(Ruhr University Bochum)*, Fabian Ising *(Münster University of Applied Sciences)*,
  Vladislav Mladenov, Christian Mainka *(Ruhr University Bochum)*,
  Sebastian Schinzel *(Münster University of Applied Sciences)*, Jörg Schwenk *(Ruhr University Bochum)*

Session 1B: Cryptographic Primitives

- **Omniring: Scaling Private Payments Without Trusted Setup: Formal Foundations and a Construction of Ring Confidential Transactions with Log-size Proofs** 31
  Russell W. F. Lai, Viktoria Ronge *(Friedrich-Alexander University Erlangen-Nuremberg)*,
  Tim Ruffing *(Blockstream)*,
  Dominique Schröder, Sri Aravinda Krishnan Thyagarajan *(Friedrich-Alexander University Erlangen-Nuremberg)*, Jiafan Wang *(Chinese University of Hong Kong)*
- **WI Is Not Enough: Zero-Knowledge Contingent (Service) Payments Revisited** 49
  Georg Fuchsbauer *(Inria, École normale supérieure, CNRS and PSL)*

Session 1C: Cloud Security I

- **A Machine-Checked Proof of Security for AWS Key Management Service** 63
  José Bacelar Almeida *(University of Minho and INESC TEC)*,
  Manuel Barbosa *(University of Porto (FCUP) and INESC TEC)*,
  Gilles Barthe *(IMDEA Software Institute and MPI-SP)*,
  Matthew Campagna, Ernie Cohen *(Amazon Web Services)*, Benjamin Gregoire *(Inria)*,
  Vitor Pereira, Bernardo Portela *(University of Porto (FCUP) and INESC TEC)*,
  Pierre-Yves Strub *(École Polytechnique)*, Serdar Tasiran *(Amazon Web Services)*
- **Mitigating Leakage in Secure Cloud-Hosted Data Structures: Volume-Hiding for Multi-Maps via Hashing** 79
  Sarvar Patel *(Google LLC)*, Giuseppe Persiano *(University of Salerno)*, Kevin Yeo *(Google LLC)*,
  Moti Yung *(Google LLC and Columbia University)*

Session 1D: Forensics

- **The Next 700 Policy Miners: A Universal Method for Building Policy Miners** 95
  Carlos Cotrini, Luca Corinzia, Thilo Weghorn, David Basin *(ETH Zürich)*
- **Towards Continuous Access Control Validation and Forensics** 113
  Chengcheng Xiang, Yudong Wu, Bingyu Shen, Mingyao Shen, Haochen Huang
  (University of California, San Diego), Tianyin Xu *(University of Illinois Urbana-Champaign)*,
  Yuanyuan Zhou, Cindy Moore *(University of California, San Diego)*,
  Xinxin Jin, Tianwei Sheng *(Whova, Inc.)*

Session 1E: Privacy I

- **Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices** 131
  Hooman Mohajeri Moghaddam, Gunes Acar, Ben Burgess, Arunesh Mathur,
  Danny Yuxing Huang *(Princeton University)*, Nick Feamster *(Princeton University & University of Chicago)*,
  Edward W. Felten, Prateek Mittal, Arvind Narayanan *(Princeton University)*

- **Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing** 149
  Ben Weinshel, Miranda Wei *(University of Chicago)*, Mainack Mondal *(IIT Kharagpur and University of Chicago)*,
  Euirim Choi, Shawn Shan, Claire Dolin *(University of Chicago)*, Michelle L. Mazurek *(University of Maryland)*,
  Blase Ur *(University of Chicago)*

Session 2A: Side Channels I

- **Page Cache Attacks** 167
  Daniel Gruss, Erik Kraft *(Graz University of Technology)*, Trishita Tiwari *(Boston University)*,
  Michael Schwarz *(Graz University of Technology)*, Ari Trachtenberg *(Boston University)*,
  Jason Hennessey *(NetApp)*, Alex Ionescu *(CrowdStrike)*, Anders Fogh *(Intel Corporation)*

- **Hardware-Backed Heist: Extracting ECDSA Keys from Qualcomm's TrustZone** 181
  Keegan Ryan *(University of California, San Diego & NCC Group)*

- **VoltJockey: Breaching TrustZone by Software-Controlled Voltage Manipulation over Multi-core Frequencies** 195
  Pengfei Qiu *(Tsinghua University & University of Maryland)*,
  Dongsheng Wang, Yongqiang Lyu *(Tsinghua University)*, Gang Qu *(University of Maryland)*

- **Principled Unearthing of TCP Side Channel Vulnerabilities** 211
  Yue Cao, Zhongjie Wang, Zhiyun Qian, Chengyu Song *(University of California, Riverside)*,
  Srikanth V. Krishnamurthy *(University of California, Riverside)*,
  Paul Yu *(U.S. Army Combat Capabilities Development Command Army Research Laboratory)*

Session 2B: ML Security I

- **Neural Network Inversion in Adversarial Setting via Background Knowledge Alignment** 225
  Ziqi Yang, Jiyi Zhang, Ee-Chien Chang, Zhenkai Liang *(National University of Singapore)*

- **Privacy Risks of Securing Machine Learning Models against Adversarial Examples** 241
  Liwei Song *(Princeton University)*, Reza Shokri *(National University of Singapore)*,
  Prateek Mittal *(Princeton University)*

- **MemGuard: Defending against Black-Box Membership Inference Attacks via Adversarial Examples** 259
  Jinyuan Jia *(Duke University)*,
  Ahmed Salem, Michael Backes, Yang Zhang *(CISPA Helmholtz Center for Information Security)*,
  Neil Zhenqiang Gong *(Duke University)*

- **Procedural Noise Adversarial Examples for Black-Box Attacks on Deep Convolutional Networks** 275
  Kenneth T. Co, Luis Muñoz-González, Sixte de Maupeou, Emil C. Lupu *(Imperial College London)*

Session 2C: Secure Computing I

- **Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation** 291
  Elette Boyle *(IDC Herzliya)*, Geoffroy Couteau *(Karlsruhe Institute of Technology)*,
  Niv Gilboa *(Ben Gurion University)*, Yuval Ishai *(Technion)*, Lisa Kohl *(Karlsruhe Institute of Technology)*,
  Peter Rindal *(Visa Research)*, Peter Scholl *(Aarhus University)*

- **Endemic Oblivious Transfer** 309
  Daniel Mansy, Peter Rindal *(VISA Research)*

- **LevioSA: Lightweight Secure Arithmetic Computation** 327
Carmit Hazay *(Bar-Ilan University)*, Yuval Ishai *(Technion)*, Antonio Marcedone *(Keybase Inc)*,
Muthuramakrishnan Venkitasubramaniam *(University of Rochester)*

- **Onion Ring ORAM: Efficient Constant Bandwidth Oblivious RAM from (Leveled) TFHE** 345
Hao Chen *(Microsoft Research)*, Ilaria Chillotti *(KU Leuven)*,
Ling Ren *(University of Illinois at Urbana-Champaign)*

Session 2D: Encryption (Searchable, Updatable, Homomorphic, etc.)

- **Encrypted Databases: New Volume Attacks against Range Queries** 361
Zichen Gui, Oliver Johnson *(University of Bristol)*, Bogdan Warinschi *(University of Bristol & Dfinity)*

- **Updatable Oblivious Key Management for Storage Systems** 379
Stanislaw Jarecki *(University of California, Irvine)*, Hugo Krawczyk *(Algorand Foundation)*,
Jason Resch *(Independent)*

- **Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference** 395
Hao Chen, Wei Dai *(Microsoft Research)*, Miran Kim *(UT Health Science Center at Houston)*,
Yongsoo Song *(Microsoft Research)*

- **Traceback for End-to-End Encrypted Messaging** 413
Nirvan Tyagi *(Cornell University)*, Ian Miers *(Cornell Tech & University of Maryland)*,
Thomas Ristenpart *(Cornell Tech)*

Session 2E: Internet Security

- **SICO: Surgical Interception Attacks by Manipulating BGP Communities** 431
Henry Birge-Lee, Liang Wang, Jennifer Rexford, Prateek Mittal *(Princeton University)*

- **Just the Tip of the Iceberg: Internet-Scale Exploitation of Routers for Cryptojacking** 449
Hugo L. J. Bijmans, Tim M. Booij, Christian Doerr *(TU Delft)*

- **Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet** 465
Matthew Luckie *(University of Waikato)*, Robert Beverly *(Naval Postgraduate School)*,
Ryan Koga, Ken Keys *(University of California, San Diego)*, Joshua A. Kroll *(Naval Postgraduate School)*,
k claffy *(University of California, San Diego)*

- **Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations** 481
Sazzadur Rahaman *(Virginia Tech)*, Gang Wang *(University of Illinois at Urbana-Champaign)*,
Danfeng (Daphne) Yao *(Virginia Tech)*

Session 3A: Fuzzing: Methods and Applications

- **Matryoshka: Fuzzing Deeply Nested Branches** 499
Peng Chen *(ByteDance AI Lab)*, Jianzhong Liu *(ShanghaiTech University)*,
Hao Chen *(University of California, Davis)*

- **Intriguer: Field-Level Constraint Solving for Hybrid Fuzzing** 515
Mingi Cho, Seoyoung Kim, Taekyoung Kwon *(Yonsei University)*

- **Learning to Fuzz from Symbolic Execution with Application to Smart Contracts** 531
Jingxuan He, Mislav Balunović, Nodar Ambroladze, Petar Tsankov, Martin Vechev *(ETH Zurich)*

Session 3B: Blockchain I

- **HyperService: Interoperability and Programmability Across Heterogeneous Blockchains**.... 549
  Zhuotao Liu *(University of Illinois at Urbana-Champaign & HyperService Consortium)*,
  Yangxi Xiang *(Beijing University of Posts and Telecommunications)*, Jian Shi *(Case Western Reserve University)*,
  Peng Gao *(University of California, Berkeley)*, Haoyu Wang *(Beijing University of Posts and Telecommunications)*,
  Xusheng Xiao *(Case Western Reserve University & HyperService Consortium)*,
  Bihan Wen *(Nanyang Technological University)*,
  Yih-Chun Hu *(University of Illinois at Urbana-Champaign & HyperService Consortium)*
- **MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol**.................... 567
  Muhammed F. Esgin *(Monash University & Data61, CSIRO)*,
  Raymond K. Zhao, Ron Steinfeld, Joseph K. Liu *(Monash University)*, Dongxi Liu *(Data61, CSIRO)*
- **Prism: Deconstructing the Blockchain to Approach Physical Limits**.................... 585
  Vivek Bagaria *(Stanford University)*, Sreeram Kannan *(University of Washington at Seattle)*,
  David Tse *(Stanford University)*, Giulia Fanti *(Carnegie Mellon University)*,
  Pramod Viswanath *(University of Illinois at Urbana-Champaign)*

Session 3C: Secure Computing II

- **Securely Sampling Biased Coins with Applications to Differential Privacy**.................... 603
  Jeffrey Champion, abhi shelat, Jonathan Ullman *(Northeastern University)*
- **Stormy: Statistics in Tor by Measuring Securely** 615
  Ryan Wails, Aaron Johnson *(U.S. Naval Research Laboratory)*, Daniel Starin *(Perspecta Labs)*,
  Arkady Yerukhimovich *(George Washington University)*, S. Dov Gordon *(George Mason University)*
- **Efficient Publicly Verifiable 2PC over a Blockchain with Applications to Financially-Secure Computations**.................... 633
  Ruiyu Zhu, Changchang Ding, Yan Huang *(Indiana University)*

Session 3D: Formal Analysis I

- **A Formal Treatment of Deterministic Wallets** 651
  Poulami Das, Sebastian Faust *(TU Darmstadt)*, Julian Loss *(Ruhr-University Bochum)*
- **5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol** 669
  Syed Rafiul Hussain *(Purdue University)*, Mitziu Echeverria *(University of Iowa)*,
  Imtiaz Karim *(Purdue University)*, Omar Chowdhury *(University of Iowa)*, Elisa Bertino *(Purdue University)*
- **Verified Verifiers for Verifying Elections**.................... 685
  Thomas Haines *(Norwegian University of Science and Technology)*,
  Rajeev Goré, Mukesh Tiwari *(Australian National University)*

Session 3E: Privacy II

- **Analyzing Subgraph Statistics from Extended Local Views with Decentralized Differential Privacy** 703
  Haipei Sun *(Qatar Computing Research Institute)*, Xiaokui Xiao *(National University of Singapore)*,
  Issa Khalil *(Qatar Computing Research Institute)*, Yin Yang *(Hamad Bin Khalifa University)*,
  Zhan Qin *(Zhejiang University)*, Hui (Wendy) Wang *(Stevens Institute of Technology)*,
  Ting Yu *(Qatar Computing Research Institute)*
- **How to Accurately and Privately Identify Anomalies** 719
  Hafiz Asif, Periklis A. Papakonstantinou, Jaideep Vaidya *(Rutgers University)*
- **Differentially Private Nonparametric Hypothesis Testing**.................... 737
  Simon Couch, Zeki Kazan, Kaiyan Shi, Andrew Bray, Adam Groce *(Reed College)*

Session 4A: Side Channels II

- **ZombieLoad: Cross-Privilege-Boundary Data Sampling** 753
  Michael Schwarz, Moritz Lipp *(Graz University of Technology)*, Daniel Moghimi *(Worcester Polytechnic Institute)*, Jo Van Bulck *(imec-DistriNet, KU Leuven)*, Julian Stecklina, Thomas Prescher *(Cyberus Technology)*, Daniel Gruss *(Graz University of Technology)*
- **Fallout: Leaking Data on Meltdown-resistant CPUs** 769
  Claudio Canella *(Graz University of Technology)*, Daniel Genkin *(University of Michigan)*, Lukas Giner, Daniel Gruss *(Graz University of Technology)*, Moritz Lipp *(Graz University of Technology)*, Marina Minkin *(University of Michigan)*, Daniel Moghimi *(Worcester Polytechnic Institute)*, Frank Piessens *(imec-DistriNet, KU Leuven)*, Michael Schwarz *(Graz University of Technology)*, Berk Sunar *(Worcester Polytechnic Institute)*, Jo Van Bulck *(imec-DistriNet, KU Leuven)*, Yuval Yarom *(University of Adelaide & Data61)*
- **SMoTherSpectre: Exploiting Speculative Execution through Port Contention** 785
  Atri Bhattacharyya *(École Polytechnique Fédérale de Lausanne)*, Alexandra Sandulescu, Matthias Neugschwandtner, Alessandro Sorniotti *(IBM Research - Zurich)*, Babak Falsafi, Mathias Payer *(École Polytechnique Fédérale de Lausanne)*, Anil Kurmus *(IBM Research - Zurich)*

Session 4B: Blockchain II

- **Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks** 801
  Christoph Egger *(Friedrich-Alexander University Erlangen-Nuremberg)*, Pedro Moreno-Sanchez, Matteo Maffei *(TU Wien)*
- **Erlay: Efficient Transaction Relay for Bitcoin** 817
  Gleb Naumenko *(University of British Columbia)*, Gregory Maxwell *(Independent)*, Pieter Wuille *(Blockstream)*, Alexandra Fedorova, Ivan Beschastnikh *(University of British Columbia)*
- **Power Adjusting and Bribery Racing: Novel Mining Attacks in the Bitcoin System** 833
  Shang Gao, Zecheng Li, Zhe Peng, Bin Xiao *(The Hong Kong Polytechnic University)*

Session 4C: Secure Computing III

- **A High-Assurance Evaluator for Machine-Checked Secure Multiparty Computation** 851
  Karim Eldefrawy *(SRI International)*, Vitor Pereira *(INESC TEC & FC Universidade do Porto)*
- **Practical Fully Secure Three-Party Computation via Sublinear Distributed Zero-Knowledge Proofs** 869
  Elette Boyle *(IDC Herzliya)*, Niv Gilboa *(Ben-Gurion University)*, Yuval Ishai *(Technion)*, Ariel Nof *(Bar-Ilan University)*
- **HoneyBadgerMPC and AsynchroMix: Practical Asynchronous MPC and its Application to Anonymous Communication** 887
  Donghang Lu *(Purdue University)*, Thomas Yurek, Samarth Kulshreshtha, Rahul Govind *(University of Illinois at Urbana-Champaign)*, Aniket Kate *(Purdue University)*, Andrew Miller *(University of Illinois at Urbana-Champaign)*

Session 4D: Formal Analysis II

- **Exploiting Symmetries When Proving Equivalence Properties for Security Protocols** 905
  Vincent Cheval, Steve Kremer, Itsaka Rakotonirina *(INRIA Nancy Grand-Est & LORIA)*
- **Are These Pairing Elements Correct? Automated Verification and Applications** 923
  Susan Hohenberger *(Johns Hopkins University)*, Satyanarayana Vusirikala *(University of Texas at Austin)*
- **Post-Collusion Security and Distance Bounding** 941
  Sjouke Mauw *(University of Luxembourg & SnT)*, Zach Smith *(University of Luxembourg)*, Jorge Toro-Pozo *(ETH Zurich)*, Rolando Trujillo-Rasua *(School of Information Technology, Deakin University)*

Session 4E: Privacy III

- **Five Years of the Right to be Forgotten** 959
  Theo Bertram, Elie Bursztein, Stephanie Caro, Hubert Chao, Rutledge Chin Feman, Peter Fleischer, Albin Gustafsson, Jess Hemerly, Chris Hibbert, Luca Invernizzi, Lanah Kammourieh Donnelly, Jason Ketover,Jay Laefer, Paul Nicholas, Yuan Niu, Harjinder Obhi, David Price, Andrew Strait, Kurt Thomas, Al Verney *(Google, Inc.)*

- **(Un)informed Consent: Studying GDPR Consent Notices in the Field** 973
  Christine Utz, Martin Degeling, Sascha Fahl *(Ruhr-Universität Bochum)*,
  Florian Schaub *(University of Michigan)*, Thorsten Holz *(Ruhr-Universität Bochum)*

- **Moving Beyond Set-It-And-Forget-It Privacy Settings on Social Media** 991
  Mainack Mondal *(IIT Kharagpur & University of Chicago)*,
  Günce Su Yilmaz, Noah Hirsch *(University of Chicago)*,
  Mohammad Taha Khan *(University of Illinois at Chicago)*, Michael Tang *(University of Chicago)*,
  Christopher Tran *(University of Illinois at Chicago)*, Chris Kanich *(University of Illinois at Chicago)*,
  Blase Ur *(University of Chicago)*, Elena Zheleva *(University of Illinois at Chicago)*

Session 5A: Software Security

- **Binary Control-Flow Trimming** 1009
  Masoud Ghaffarinia, Kevin W. Hamlen *(University of Texas at Dallas)*

- **Program-mandering: Quantitative Privilege Separation** 1023
  Shen Liu, Dongrui Zeng, Yongzhe Huang, Frank Capobianco *(Pennsylvania State University)*,
  Stephen McCamant *(University of Minnesota)*, Trent Jaeger, Gang Tan *(Pennsylvania State University)*

Session 5B: Protocols

- **Flexible Byzantine Fault Tolerance** 1041
  Dahlia Malkhi *(Calibra)*, Kartik Nayak *(Duke University)*,
  Ling Ren *(University of Illinois at Urbana-Champaign)*

- **Distributed Vector-OLE: Improved Constructions and Implementation** 1055
  Phillipp Schoppmann *(Humboldt-Universität zu Berlin)*, Adrià Gascón *(Google)*,
  Leonie Reichert *(Humboldt-Universität zu Berlin)*, Mariana Raykova *(Google)*

Session 5C: Cloud Security II

- **Houdini's Escape: Breaking the Resource Rein of Linux Control Groups** 1073
  Xing Gao *(University of Memphis)*, Zhongshu Gu *(IBM Research)*, Zhengfa Li *(Independent Researcher)*,
  Hani Jamjoom *(IBM Research)*, Cong Wang *(Old Dominion University)*

- **Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation** 1087
  Robert Buhren *(Technische Universität Berlin)*, Christian Werling *(Hasso Plattner Institute)*,
  Jean-Pierre Seifert *(Technische Universität Berlin)*

Session 5D: SDN Security

- **An In-depth Look Into SDN Topology Discovery Mechanisms: Novel Attacks and Practical Countermeasures** 1101
  Eduard Marin *(University of Birmingham (UK) and imec-COSIC, KU Leuven (Belgium))*,
  Nicola Bucciol, Mauro Conti *(University of Padua)*

- **Proof-Carrying Network Code** 1115
  Christian Skalka, John Ring, David Darias *(University of Vermont)*,
  Minseok Kwon, Sahil Gupta, Kyle Diller *(Rochester Institute of Technology)*,
  Steffen Smolka, Nate Foster *(Cornell University)*

Session 5E: Fingerprinting

- **Triplet Fingerprinting: More Practical and Portable Website Fingerprinting with N-shot Learning** 1131
  Payap Sirinam *(Navaminda Kasatriyadhiraj Royal Air Force Academy)*,
  Nate Mathews, Mohammad Saidur Rahman, Matthew Wright *(Rochester Institute of Technology)*
- **DeMiCPU: Device Fingerprinting with Magnetic Signals Radiated by CPU** 1149
  Yushi Cheng, Xiaoyu Ji, Juchuan Zhang, Wenyuan Xu *(Zhejiang University)*,
  Yi-Chao Chen *(University of Texas at Austin)*

Session 6A: Biometrics Security

- **Multisketches: Practical Secure Sketches Using Off-the-Shelf Biometric Matching Algorithms** 1171
  Rahul Chatterjee *(University of Wisconsin–Madison)*, M. Sadegh Riazi *(University of California San Diego)*,
  Tanmoy Chowdhury, Emanuela Marasco *(George Mason University)*,
  Farinaz Koushanfar *(University of California San Diego)*, Ari Juels *(Cornell Tech)*
- **28 Blinks Later: Tackling Practical Challenges of Eye Movement Biometrics** 1187
  Simon Eberz, Giulio Lovisotto, Kasper B. Rasmussen *(University of Oxford)*, Vincent Lenders *(armasuisse)*,
  Ivan Martinovic *(University of Oxford)*
- **Velody: Nonlinear Vibration Challenge-Response for Resilient User Authentication** 1201
  Jingjie Li, Kassem Fawaz, Younghyun Kim *(University of Wisconsin-Madison)*
- **The Catcher in the Field: A Fieldprint based Spoofing Detection for Text-Independent Speaker Verification** 1215
  Chen Yan, Yan Long, Xiaoyu Ji, Wenyuan Xu *(Zhejiang University)*

Session 6B: ML Security II

- **QUOTIENT: Two-Party Secure Neural Network Training and Prediction** 1231
  Nitin Agrawal *(University of Oxford)*, Ali Shahin Shamsabadi *(Queen Mary University of London)*,
  Matt J. Kusner *(University of Oxford & The Alan Turing Institute)*,
  Adrià Gascón *(University of Warwick & The Alan Turing Institute)*
- **Quantitative Verification of Neural Networks and Its Security Applications** 1249
  Teodora Baluta, Shiqi Shen *(National University of Singapore)*, Shweta Shinde *(University of California, Berkeley)*,
  Kuldeep S. Meel, Prateek Saxena *(National University of Singapore)*
- **ABS: Scanning Neural Networks for Back-doors by Artificial Brain Stimulation** 1265
  Yingqi Liu, Wen-Chuan Lee, Guanhong Tao *(Purdue University)*, Shiqing Ma *(Rutgers University)*,
  Yousra Aafer, Xiangyu Zhang *(Purdue University)*
- **Lifelong Anomaly Detection Through Unlearning** 1283
  Min Du, Zhi Chen *(University of California, Berkeley)*, Chang Liu *(Citadel Securities)*,
  Rajvardhan Oak, Dawn Song *(University of California, Berkeley)*

Session 6C: Secure Computing VI

- **Transparency Logs via Append-Only Authenticated Dictionaries** 1299
  Alin Tomescu *(Massachusetts Institute of Technology)*, Vivek Bhupatiraju *(Lexington High School & MIT PRIMES)*,
  Dimitrios Papadopoulos *(Hong Kong University of Science and Technology)*,
  Charalampos Papamanthou *(University of Maryland)*, Nikos Triandopoulos *(Stevens Institute of Technology)*,
  Srinivas Devadas *(Massachusetts Institute of Technology)*
- **Probabilistic Data Structures in Adversarial Environments** 1317
  David Clayton, Christopher Patton, Thomas Shrimpton *(University of Florida)*
- **Make Some ROOM for the Zeros: Data Sparsity in Secure Distributed Machine Learning** .. 1335
  Phillipp Schoppmann *(Humboldt-Universität zu Berlin)*,
  Adrià Gascón *(The Alan Turing Institute / University of Warwick)*, Mariana Raykova *(Google)*,
  Benny Pinkas *(Bar-Ilan University)*
- **PIEs: Public Incompressible Encodings for Decentralized Storage** 1351
  Ethan Cecchetti *(Cornell University)*, Ben Fisch *(Stanford University)*, Ian Miers *(Cornell Tech)*,
  Ari Juels *(Jacobs Institute, Cornell Tech)*

Session 6D: Cyber Thread

- **Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyber Threats within Enterprise** 1777
  Fucheng Liu *(Institute of Information Engineering, CAS & School of Cyber Security, University of Chinese Academy of Sciences)*,
  Yu Wen, Dongxue Zhang *(Institute of Information Engineering, Chinese Academy of Sciences)*,
  Xihe Jiang *(Institute of Information Engineering, CAS & School of Cyber Security, University of Chinese Academy of Sciences)*,
  Xinyu Xing *(The Pennsylvania State University & JD Security Research Center)*,
  Dan Meng *(Institute of Information Engineering, Chinese Academy of Sciences)*
- **POIROT: Aligning Attack Behavior with Kernel Audit Records for Cyber Threat Hunting** 1795
  Sadegh M. Milajerdi *(University of Illinois at Chicago)*, Birhanu Eshete *(University of Michigan-Dearborn)*,
  Rigel Gjomemo, V.N. Venkatakrishnan *(University of Illinois at Chicago)*
- **Effective and Light-Weight Deobfuscation and Semantic-Aware Attack Detection for PowerShell Scripts** 1831
  Zhenyuan Li *(Zhejiang University)*, Qi Alfred Chen *(University of California, Irvine)*,
  Chunlin Xiong *(Zhejiang University)*, Yan Chen *(Northwestern University)*,
  Tiantian Zhu *(Zhejiang University of Technology)*, Hai Yang *(MagicShield Inc)*
- **MalMax: Multi-Aspect Execution for Automated Dynamic Web Server Malware Analysis** 1849
  Abbas Naderi-Afooshteh, Yonghwi Kwon, Anh Nguyen-Tuong *(University of Virginia)*,
  Ali Razmjoo-Qalaei, Mohammad-Reza Zamiri-Gourabi *(ZDResearch)*, Jack W. Davidson *(University of Virginia)*

Session 6E: Passwords and Accounts

- **How to (not) Share a Password: Privacy Preserving Protocols for Finding Heavy Hitters with Adversarial Behavior** 1369
  Moni Naor *(Weizmann Institute of Science)*, Benny Pinkas *(Bar-Ilan University)*,
  Eyal Ronen *(Tel Aviv University & KU Leuven)*
- **Protocols for Checking Compromised Credentials** 1387
  Lucy Li, Bijeeta Pal *(Cornell University)*, Junade Ali, Nick Sullivan *(Cloudflare Inc.)*,
  Rahul Chatterjee *(University of Wisconsin-Madison & Cornell Tech)*, Thomas Ristenpart *(Cornell Tech)*
- **User Account Access Graphs** 1405
  Sven Hammann *(ETH Zurich)*, Saša Radomirović *(University of Dundee)*, Ralf Sasse, David Basin *(ETH Zurich)*
- **Detecting Fake Accounts in Online Social Networks at the Time of Registrations** 1423
  Dong Yuan, Yuanli Miao *(Tsinghua University)*, Neil Zhenqiang Gong *(Duke University)*,
  Zheng Yang, Qi Li *(Tsinghua University)*, Dawn Song *(University of California, Berkeley)*,
  Qian Wang *(Wuhan University)*, Xiao Liang *(Tencent)*

Session 7A: Internet of Things

- **Charting the Attack Surface of Trigger-Action IoT Platforms** 1439
  Qi Wang, Pubali Datta *(University of Illinois at Urbana-Champaign)*, Wei Yang *(The University of Texas at Dallas)*,
  Si Liu, Adam Bates, Carl A. Gunter *(University of Illinois at Urbana-Champaign)*
- **Peeves: Physical Event Verification in Smart Homes** 1455
  Simon Birnbach, Simon Eberz, Ivan Martinovic *(University of Oxford)*
- **Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps** 1469
  Chaoshun Zuo, Haohuang Wen, Zhiqiang Lin, Yinqian Zhang *(Ohio State University)*

Session 7B: Blockchain III

- **Balance: Dynamic Adjustment of Cryptocurrency Deposits** 1485
  Dominik Harz, Lewis Gudgeon, Arthur Gervais, William J. Knottenbelt *(Imperial College London)*

- **TokenScope: Automatically Detecting Inconsistent Behaviors of Cryptocurrency Tokens in Ethereum** 1503
  Ting Chen, Yufei Zhang, Zihao Li *(University of Electronic Science and Technology of China)*,
  Xiapu Luo *(The Hong Kong Polytechnic University)*, Ting Wang *(The Pennsylvania State University)*,
  Rong Cao, Xiuzhuo Xiao, Xiaosong Zhang *(University of Electronic Science and Technology of China)*
- **Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware** 1521
  Iddo Bentov, Yan Ji, Fan Zhang *(Cornell Tech)*, Lorenz Breidenbach *(ETH Zürich & Cornell Tech)*,
  Philip Daian, Ari Juels *(Cornell Tech)*

Session 7C: Secure Computing V

- **Efficient MPC via Program Analysis: A Framework for Efficient Optimal Mixing** 1539
  Muhammad Ishaq *(University of Edinburgh)*, Ana L. Milanova *(Rensselaer Polytechnic Institute)*,
  Vassilis Zikas *(University of Edinburgh)*
- **Two-Thirds Honest-Majority MPC for Malicious Adversaries at Almost the Cost of Semi-Honest** 1557
  Jun Furukawa *(NEC Israel Research Center)*, Yehuda Lindell *(Bar-Ilan University & Unbound Tech)*
- **Fast Actively Secure Five-Party Computation with Security Beyond Abort** 1573
  Megha Byali *(Indian Institute of Science)*, Carmit Hazay *(Bar-Ilan University)*,
  Arpita Patra, Swati Singla *(Indian Institute of Science)*

Session 7D: Formal Analysis III

- **Signed Cryptographic Program Verification with Typed CryptoLine** 1591
  Yu-Fu Fu *(Academia Sinica)*, Jiaxiang Liu, Xiaomu Shi *(Shenzhen University)*,
  Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang *(Academia Sinica)*
- **Machine-Checked Proofs for Cryptographic Standards: Indifferentiability of Sponge and Secure High-Assurance Implementations of SHA-3** 1607
  JoséBacelar Almeida *(Universidade do Minho & INESC-TEC)*,
  Cécile Baritel-Ruet *(UniversitéCôte d'Azur & Inria Sophia-Antipolis)*,
  Manuel Barbosa *(Universidade do Porto & INESC-TEC)*, Gilles Barthe *(MPI-SP & IMDEA Software Institute)*,
  François Dupressoir *(University of Surrey & University of Bristol)*, Benjamin Grégoire *(Inria Sophia-Antipolis)*,
  Vincent Laporte *(Inria)*, Tiago Oliveira *(Universidade do Porto & INESC-TEC & FCUP)*,
  Alley Stoughton *(Boston University)*, Pierre-Yves Strub *(École Polytechnique)*
- **VeriSketch: Synthesizing Secure Hardware Designs with Timing-Sensitive Information Flow Properties** 1623
  Armaiti Ardeshiricham, Yoshiki Takashima, Sicun Gao, Ryan Kastner
  (University of California, San Diego)

Session 7E: Privacy-Preserving Techniques

- **SEEM*less*: Secure End-to-End Encrypted Messaging with *less* Trust** 1639
  Melissa Chase *(Microsoft Research)*, Apoorvaa Deshpande *(Brown University)*,
  Esha Ghosh *(Microsoft Research)*, Harjasleen Malvai *(Cornell University)*
- **PrivDPI: Privacy-Preserving Encrypted Traffic Inspection with Reusable Obfuscated Rules** 1657
  Jianting Ning *(Fujian Normal University & National University of Singapore)*,
  Geong Sen Poh *(Trustwave & NUS-Singtel Cyber Security Lab)*,
  Jia-Ch'ng Loh, Jason Chia *(NUS-Singtel Cyber Security Lab)*,
  Ee-Chien Chang *(National University of Singapore)*
- **Updatable Anonymous Credentials and Applications to Incentive Systems** 1671
  Johannes Blömer, Jan Bobolz, Denis Diemert, Fabian Eidens *(Paderborn University)*

Keynote

- **Hardware-assisted Trusted Execution Environments: Look Back, Look Ahead** 1687
  N. Asokan *(University of Waterloo)*

Session 8A: Attack II

- **Gollum: Modular and Greybox Exploit Generation for Heap Overflows in Interpreters** 1689
  Sean Heelan, Tom Melham, Daniel Kroening *(University of Oxford)*
- **SLAKE: Facilitating Slab Manipulation for Exploiting Vulnerabilities in the Linux Kernel** 1707
  Yueqi Chen, Xinyu Xing *(Pennsylvania State University)*

Session 8B: TEE I

- **SecTEE: A Software-based Approach to Secure Enclave Architecture Using TEE** 1723
  Shijun Zhao *(Institute of Software Chinese Academy of Sciences)*, Qianying Zhang *(Capital Normal University)*,
  Yu Qin, Wei Feng, Dengguo Feng *(Institute of Software Chinese Academy of Sciences)*
- **A Tale of Two Worlds: Assessing the Vulnerability of Enclave Shielding Runtimes** 1741
  Jo Van Bulck *(KU Leuven)*,
  David Oswald, Eduard Marin, Abdulla Aldoseri, Flavio D. Garcia, Frank Piessens *(University of Birmingham)*

Session 8C: Blockchain VI

- **zkay: Specifying and Enforcing Data Privacy in Smart Contracts** 1759
  Samuel Steffen, Benjamin Bichsel, Mario Gersbach, Noa Melchior, Petar Tsankov, Martin Vechev *(ETH Zurich)*
- **Privacy Aspects and Subliminal Channels in Zcash** 1813
  Alex Biryukov, Daniel Feher, Giuseppe Vitto *(University of Luxembourg)*

Session 8D: Language Security

- **Where Does It Go? Refining Indirect-Call Targets with Multi-Layer Type Analysis** 1867
  Kangjie Lu *(University of Minnesota, Twin Cities)*, Hong Hu *(Georgia Institute of Technology)*
- **Different is Good: Detecting the Use of Uninitialized Variables through Differential Replay** 1883
  Mengchen Cao, Xiantong Hou, Tao Wang, Hunter Qu *(Orion Security Lab, Alibaba Group)*,
  Yajin Zhou *(Zhejiang University)*, Xiaolong Ba, Fuwei Wang *(Orion Security Lab, Alibaba Group)*

Session 8E: Web Security

- **HideNoSeek: Camouflaging Malicious JavaScript in Benign ASTs** 1899
  Aurore Fass, Michael Backes, Ben Stock *(CISPA Helmholtz Center for Information Security)*
- **Your Cache Has Fallen: Cache-Poisoned Denial-of-Service Attack** 1915
  Hoai Viet Nguyen, Luigi Lo Iacono *(Cologne University of Applied Sciences)*,
  Hannes Federrath *(University of Hamburg)*

Session 9A: User Study

- **"I don't see why I would ever want to use it": Analyzing the Usability of Popular Smartphone Password Managers** 1937
  Sunyoung Seiler-Hwang, Patricia Arias-Cabarcos *(University of Mannheim)*,
  Andrés Marín, Florina Almenares, Daniel Díaz-Sánchez *(University Carlos III of Madrid)*,
  Christian Becker *(University of Mannheim)*
- **Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues** 1955
  Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili *(Arizona State University)*,
  Ziming Zhao *(Rochester Institute of Technology)*, Adam Doupé *(Arizona State University)*,
  Gail-Joon Ahn *(Arizona State University and Samsung Research)*
- **A Usability Evaluation of Let's Encrypt and Certbot: Usable Security Done Right** 1971
  Christian Tiefenau *(University of Bonn)*,

Emanuel von Zezschwitz, Maximilian Häring *(University of Bonn & Fraunhofer FKIE)*,
Katharina Krombholz *(CISPA Helmholtz Center)*, Matthew Smith *(University of Bonn & Fraunhofer FKIE)*

Session 9B: ML Security III

- **Seeing isn't Believing: Towards More Robust Adversarial Attack Against Real World Object Detectors** 1989
  Yue Zhao, Hong Zhu, Ruigang Liang, Qintao Shen *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*,
  Shengzhi Zhang *(Metropolitan College, Boston University)*,
  Kai Chen *(Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences)*
- **AdVersarial: Perceptual Ad Blocking meets Adversarial Machine Learning** 2005
  Florian Tramèr *(Stanford University)*, Pascal Dupré *(CISPA Helmholtz Center for Information Security)*,
  Gili Rusak *(Stanford University)*,
  Giancarlo Pellegrino *(Stanford University, CISPA Helmholtz Center for Information Security)*,
  Dan Boneh *(Stanford University)*
- **Attacking Graph-based Classification via Manipulating the Graph Structure** 2023
  Binghui Wang, Neil Zhenqiang Gong *(Duke University)*
- **Latent Backdoor Attacks on Deep Neural Networks** 2041
  Yuanshun Yao, Huiying Li, Haitao Zheng, Ben Y. Zhao *(University of Chicago)*

Session 9C: Zero-Knowledge Proofs

- **Succinct Arguments for Bilinear Group Arithmetic: Practical Structure-Preserving Cryptography** 2057
  Russell W. F. Lai *(Friedrich-Alexander University Erlangen-Nuremberg)*,
  Giulio Malavolta *(Carnegie Mellon University)*,
  Viktoria Ronge *(Friedrich-Alexander University Erlangen-Nuremberg)*
- **LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs** 2075
  Matteo Campanelli, Dario Fiore *(IMDEA Software Institute)*,
  Anaïs Querol *(IMDEA Software Institute & Universidad Politécnica de Madrid)*
- **Efficient Zero-Knowledge Arguments in the Discrete Log Setting, Revisited** 2093
  Max Hoffmann *(Ruhr-University Bochum)*, Michael Klooß, Andy Rupp *(Karlsruhe Institute of Technology)*
- **Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings** 2111
  Mary Maller *(University College London)*, Sean Bowe *(Electric Coin Company)*,
  Markulf Kohlweiss *(University of Edinburgh & IOHK)*, Sarah Meiklejohn *(University College London)*

Session 9D: Signatures

- **The SPHINCS$^+$ Signature Framework** 2129
  Daniel J. Bernstein *(University of Illinois at Chicago & Ruhr University Bochum)*,
  Andreas Hülsing *(Eindhoven University of Technology)*, Stefan Kölbl *(Cybercrypt)*,
  Ruben Niederhagen *(Fraunhofer SIT, Darmstadt)*, Joost Rijneveld, Peter Schwabe *(Radboud University)*
- **GALACTICS: Gaussian Sampling for Lattice-Based Constant - Time Implementation of Cryptographic Signatures, Revisited** 2147
  Gilles Barthe *(MPI-SP and IMDEA Software Institute)*, Sonia Belaïd *(CryptoExperts)*,
  Thomas Espitau *(Sorbonne Université)*, Pierre-Alain Fouque *(Université de Rennes)*,
  Mélissa Rossi *(Thales, ENS Paris, CNRS, PSL University, INRIA)*, Mehdi Tibouchi *(NTT Corporation)*
- **Seems Legit: Automated Analysis of Subtle Attacks on Protocols that Use Signatures** 2165
  Dennis Jackson *(University of Oxford)*, Cas Cremers *(CISPA Helmholtz Center for Information Security)*,
  Katriel Cohn-Gordon *(Independent Scholar)*, Ralf Sasse *(ETH Zurich)*
- **Membership Privacy for Fully Dynamic Group Signatures** 2181
  Michael Backes *(CISPA Helmholtz Center for Information Security)*,

Lucjan Hanzlik *(CISPA Helmholtz Center for Information Security & Stanford University)*,
Jonas Schneider-Bensch *(CISPA Helmholtz Center for Information Security)*

Session 9E: Web Censorship and Auditing

- **Geneva: Evolving Censorship Evasion Strategies** 2199
  Kevin Bock, George Hughey *(University of Maryland)*, Xiao Qiang *(University of California, Berkeley)*,
  Dave Levin *(University of Maryland)*
- **Conjure: Summoning Proxies from Unused Address Space** 2215
  Sergey Frolov, Jack Wampler *(University of Colorado Boulder)*,
  Sze Chuen Tan *(University of Illinois at Urbana-Champaign)*, J. Alex Halderman *(University of Michigan)*,
  Nikita Borisov *(University of Illinois at Urbana-Champaign)*, Eric Wustrow *(University of Colorado Boulder)*
- **You Shall Not Join: A Measurement Study of Cryptocurrency Peer-to-Peer Bootstrapping Techniques** 2231
  Angelique Faye Loe, Elizabeth Anne Quaglia *(Royal Holloway, University of London)*
- **SAMPL: Scalable Auditability of Monitoring Processes using Public Ledgers** 2249
  Gaurav Panwar, Roopa Vishwanathan, Satyajayant Misra, Austin Bos *(New Mexico State University)*

Session 10A: Cyberphysical Security

- **Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving** 2267
  Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi *(University of Michigan)*,
  Qi Alfred Chen *(University of California, Irvine)*, Kevin Fu, Z. Morley Mao *(University of Michigan)*
- **LibreCAN: Automated CAN Message Translator** 2283
  Mert D. Pesé, Troy Stacer, C. Andrés Campos, Eric Newberry, Dongyao Chen,
  Kang G. Shin *(University of Michigan)*
- **Trick or Heat? Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks** 2301
  Yazhou Tu *(University of Louisiana at Lafayette)*, Sara Rampazzi *(University of Michigan)*,
  Bin Hao *(University of Louisiana at Lafayette)*, Angel Rodriguez, Kevin Fu *(University of Michigan)*,
  Xiali Hei *(University of Louisiana at Lafayette)*

Session 10B: TEE II

- **OPERA: Open Remote Attestation for Intel's Secure Enclaves** 2317
  Guoxing Chen, Yinqian Zhang, Ten-Hwang Lai *(Ohio State University)*
- **Towards Memory Safe Enclave Programming with Rust-SGX** 2333
  Huibo Wang *(Baidu X-Lab & The University of Texas at Dallas)*, Pei Wang, Yu Ding, Mingshen Sun,
  Yiming Jing, Ran Duan, Long Li, Yulong Zhang, Tao Wei *(Baidu X-Lab)*, Zhiqiang Lin *(Ohio State University)*
- **LightBox: Full-stack Protected Stateful Middlebox at Lightning Speed** 2351
  Huayi Duan, Cong Wang *(City University of Hong Kong and City University of Hong Kong Shenzhen Research Institute)*, Xingliang Yuan *(Monash University)*,
  Yajin Zhou *(Zhejiang University & Alibaba-Zhejiang University Joint Institute of Frontier)*,
  Qian Wang *(Wuhan University)*,
  Kui Ren *(Zhejiang University & Alibaba-Zhejiang University Joint Institute of Frontier)*

Session 10C: Secret Sharing

- **CHURP: Dynamic-Committee Proactive Secret Sharing** 2369
  Sai Krishna Deepak Maram, Fan Zhang *(Cornell Tech)*,
  Lun Wang, Andrew Low *(University of California, Berkeley)*,
  Yupeng Zhang *(Texas A&M)*, Ari Juels *(Cornell Tech)*, Dawn Song *(University of California, Berkeley)*
- **Efficient Verifiable Secret Sharing with Share Recovery in BFT Protocols** 2387
  Soumya Basu *(Cornell University & IC3)*, Alin Tomescu *(Massachusetts Institute of Technology)*,
  Ittai Abraham *(VMware Research)*, Dahlia Malkhi *(Calibra)*,
  Michael K. Reiter *(University of North Carolina at Chapel Hill & VMware Research)*,
  Emin Gün Sirer *(Cornell University & IC3)*

- **Two-party Private Set Intersection with an Untrusted Third Party** 2403
  Phi Hung Le *(George Mason University)*, Samuel Ranellucci *(Unbound Tech)*,
  Samuel Dov Gordon *(George Mason University)*

Session 10D: Mobile Security

- **DeepIntent: Deep Icon-Behavior Learning for Detecting Intention-Behavior Discrepancy in Mobile Apps** 2421
  Shengqu Xi *(Nanjing University)*, Shao Yang, Xusheng Xiao *(Case Western Reserve University)*,
  Yuan Yao, Yayuan Xiong, Fengyuan Xu *(Nanjing University)*,
  Haoyu Wang *(Beijing University of Posts and Telecommunications)*, Peng Gao *(University of California, Berkeley)*,
  Zhuotao Liu *(University of Illinois at Urbana-Champaign)*, Feng Xu, Jian Lu *(Nanjing University)*
- **The Art and Craft of Fraudulent App Promotion in Google Play** 2437
  Mizanur Rahman *(Amazon)*, Nestor Hernandez, Ruben Recabarren *(Florida International University)*,
  Syed Ishtiaque Ahmed *(University of Toronto)*, Bogdan Carbunar *(Florida International University)*
- **CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects** 2455
  Sazzadur Rahaman, Ya Xiao, Sharmin Afrose *(Virginia Tech)*, Fahad Shaon *(University of Texas at Dallas)*,
  Ke Tian, Miles Frantz *(Virginia Tech)*, Murat Kantarcioglu *(University of Texas at Dallas)*,
  Danfeng (Daphne) Yao *(Virginia Tech)*

Session 10E: Certificates

- **Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web** 2473
  Josh Aas *(Let's Encrypt)*, Richard Barnes *(Cisco)*, Benton Case, Zakir Durumeric *(Stanford University)*,
  Peter Eckersley *(Electronic Frontier Foundation)*, Alan Flores-López *(Stanford University)*,
  J. Alex Halderman *(University of Michigan)*, Jacob Hoffman-Andrews *(Electronic Frontier Foundation)*,
  James Kasten *(University of Michigan)*, Eric Rescorla *(Mozilla)*,
  Seth Schoen, Brad Warren *(Electronic Frontier Foundation)*
- **You Are Who You Appear to Be: A Longitudinal Study of Domain Impersonation in TLS Certificates** 2489
  Richard Roberts, Yaelle Goldschlag, Rachel Walter *(University of Maryland)*,
  Taejoong Chung *(Rochester Institute of Technology)*, Alan Mislove *(Northeastern University)*,
  Dave Levin *(University of Maryland)*
- **Certificate Transparency in the Wild: Exploring the Reliability of Monitors** 2505
  Bingyu Li, Jingqiang Lin *(Chinese Academy of Sciences & University of Chinese Academy of Sciences)*,
  Fengjun Li *(University of Kansas)*, Qiongxiao Wang *(Chinese Academy of Sciences)*, Qi Li *(Tsinghua University)*,
  Jiwu Jing *(University of Chinese Academy of Sciences)*,
  Congli Wang *(Chinese Academy of Sciences & University of Chinese Academy of Sciences)*

Posters

- **POSTER: Detecting Audio Adversarial Example through Audio Modification** 2521
  Hyun Kwon, Hyunsoo Yoon *(Korea Advanced Institute of Science and Technology)*,
  Ki-Woong Park *(Sejong University)*
- **Poster: Fuzzing IoT Firmware via Multi-stage Message Generation** 2525
  Bo Yu, Pengfei Wang, Tai Yue, Yong Tang *(National University of Defense Technology)*
- **Poster: Snout – An Extensible IoT Pen-Testing Tool** 2529
  John Mikulskis, Johannes K. Becker, Stefan Gvozdenovic, David Starobinski *(Boston University)*
- **POSTER: Traffic Splitting to Counter Website Fingerprinting** 2533
  Wladimir De la Cadena *(University of Luxembourg)*, Asya Mitseva *(University of Luxembourg)*,
  Jan Pennekamp *(RWTH Aachen University)*, Jens Hiller *(RWTH Aachen University)*,
  Fabian Lanze *(Huf Secure Mobile GmbH)*, Thomas Engel *(University of Luxembourg)*,
  Klaus Wehrle *(RWTH Aachen University)*, Andriy Panchenko *(Brandenburg University of Technology)*
- **Poster: Force vs. Nudge – Comparing Users' Pattern Choices on SysPal and TinPal** 2537
  Harshal Tupsamudre, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Lodha *(TCS Research)*

- **Poster: Framework for Semi-Private Function Evaluation with Application to Secure Insurance Rate Calculation** 2541
  Daniel Günther, Ágnes Kiss, Lukas Scheidel, Thomas Schneider *(TU Darmstadt)*
- **Poster: Deployment-quality and Accessible Solutions for Cryptography Code Development** 2545
  Sazzadur Rahaman, Ya Xiao, Sharmin Afrose, Ke Tian, Miles Frantz, Na Meng *(Virginia Tech)*,
  Barton P. Miller *(University of Wisconsin-Madison)*,
  Fahad Shaon, Murat Kantarcioglu *(University of Texas at Dallas)*, Danfeng (Daphne) Yao *(Virginia Tech)*
- **Poster—Medical Protocol Security: DICOM Vulnerability Mining Based on Fuzzing Technology** 2549
  Zhiqiang Wang *(Beijing Eletronic Science and Technology Institute, State Key Laboratory of Cryptology, & State Information Center)*,
  Quanqi Li, Yazhe Wang, Biao Liu, Jianyi Zhang *(Beijing Eletronic Science and Technology Institute)*,
  Qixu Liu *(Institute of Information Engineering, Chinese Academy of Sciences)*
- **Poster: A Proof-of-Stake (PoS) Blockchain Protocol using Fair and Dynamic Sharding Management** 2553
  Daehwa Rayer Lee, Yunhee Jang *(Sungkyunkwan University)*, Hyoungshick Kim *(CSIRO Data61)*
- **Poster: Kerberoid: A Practical Android App Decompilation System with Multiple Decompilers** 2557
  Heejun Jang, Beomjin Jin *(Sungkyunkwan University)*, Sangwon Hyun *(Myongji University)*,
  Hyoungshick Kim *(Sungkyunkwan University and CSIRO Data61)*
- **Poster: A Reliable and Accountable Privacy-Preserving Federated Learning Framework using the Blockchain** 2561
  Sana Awan, Fengjun Li, Bo Luo *(University of Kansas)*, Mei Liu *(University of Kansas Medical Center)*
- **Poster: Attacking Malware Classifiers by Crafting Gradient-Attacks that Preserve Functionality** 2565
  Raphael Labaca-Castro *(Bundeswehr University Munich)*, Battista Biggio *(University of Cagliari)*,
  Gabi Dreo Rodosek *(Bundeswehr University Munich)*
- **Poster: simFIDO – FIDO2 User Authentication with simTPM** 2569
  Dhiman Chakraborty *(CISPA Helmholtz Center for Information Security & Saarland University)*,
  Sven Bugiel *(CISPA Helmholtz Center for Information Security)*
- **Poster: pFilter – Retrofitting Legacy Applications for Data Privacy** 2573
  Manish Shukla, Kumar Vidhani, Gangadhara Sirigireddy, Vijayanand Banahatti,
  Sachin Lodha *(TCS Research Lab)*
- **Poster: Towards a Framework for Assessing Vulnerabilities of Brainwave Authentication Systems** 2577
  Karen Becker, Patricia Arias-Cabarcos, Thilo Habrich *(University of Mannheim)*,
  Christian Becker *(University of Mannheim, Mannheim, Germany)*
- **Poster: Network Message Field Type Recognition** 2581
  Stephan Kleber, Frank Kargl *(Ulm University)*
- **Poster: Towards a Data Centric Approach for the Design and Verification of Cryptographic Protocols** 2585
  Luca Arnaboldi *(Newcastle University)*, Roberto Metere *(Newcastle University & The Alan Turing Institute)*
- **Poster: ÆGIS: Smart Shielding of Smart Contracts** 2589
  Christof Ferreira Torres, Mathis Baden, Robert Norvill *(University of Luxembourg)*,
  Hugo Jonker *(Open University of the Netherlands & Radbound University)*
- **Poster: Nickel to Lego – Using *Foolgle* to Create Adversarial Examples to Fool Google Cloud Speech-to-Text API** 2593
  Joon Kuy Han *(The State University of New York)*,
  Hyoungshick Kim *(Sungkyunkwan University & CSIRO Data61)*, Simon S. Woo *(Sungkyunkwan University)*
- **Poster: Using Generative Adversarial Networks for Secure Pseudorandom Number Generation** 2597
  Rajvardhan Oak *(University of California, Berkeley)*, Chaitanya Rahalkar, Dhaval Gujar *(University of Pune)*

- **Poster: Proofs of Retrievability with Low Server Storage** 2601
  Michael Hanling *(United States Naval Academy)*, Gaspard Anthoine, Jean-Guillaume Dumas, Aude Maignan, Clément Pernet *(Laboratoire Jean Kuntzmann)*, Daniel S. Roche *(United States Naval Academy)*
- **Poster: Data Quality for Security Challenges: Case Studies of Phishing, Malware and Intrusion Detection Datasets** 2605
  Rakesh M. Verma, Victor Zeng, Houtan Faridi *(University of Houston)*
- **Poster: Finding JavaScript Name Conflicts on the Web** 2609
  Mingxue Zhang, Wei Meng *(Chinese University of Hong Kong)*,
  Yi Wang *(Southern University of Science and Technology)*
- **Poster: Towards Robust Open-World Detection of Deepfakes** 2613
  Saniat Javid Sohrawardi, Akash Chintha, Bao Thai, Sovantharith Seng *(Rochester Institute of Technology)*,
  Andrea Hickerson *(University of South Carolina)*,
  Raymond Ptucha, Matthew Wright *(Rochester Institute of Technology)*
- **Poster: Understanding User's Decision to Interact with Potential Phishing Posts on Facebook using a Vignette Study** 2617
  Sovantharith Seng *(Rochester Institute of Technology)*, Huzeyfe Kocabas *(Utah State University)*,
  Mahdi Nasrullah Al-Ameen, Matthew Wright *(Rochester Institute of Technology)*
- **Poster: Adversarial Examples for Hate Speech Classifiers** 2621
  Rajvardhan Oak *(University of California, Berkeley)*
- **Poster: Evaluating Security Metrics for Website Fingerprinting** 2625
  Nate Mathews, Mohammad Saidur Rahman, Matthew Wright *(Rochester Institute of Technology)*
- **Poster: Video Fingerprinting in Tor** 2629
  Mohammad Saidur Rahman, Nate Matthews, Matthew Wright *(Rochester Institute of Technology)*
- **Poster: A First Look at the Privacy Risks of Voice Assistant Apps** 2633
  Atsuko Natatsuka *(Waseda University)*, Ryo Iijima *(Waseda University & NICT)*,
  Takuya Watanabe *(NTT Secure Platform Laboratories & Waseda University)*,
  Mitsuaki Akiyama *(NTT Secure Platform Laboratories)*, Tetsuya Sakai *(Waseda University)*,
  Tatsuya Mori *(Waseda University, NICT & RIKEN AIP)*
- **Poster: Directed Hybrid Fuzzing on Binary Code** 2637
  Juhwan Kim, Joobeom Yun *(Sejong University)*
- **Poster: On the Application of NLP to Discover Relationships between Malicious Network Entities** 2641
  Giuseppe Siracusano *(NEC Laboratories Europe)*, Martino Trevisan *(Politecnico di Torino)*,
  Roberto Gonzalez, Roberto Bifulco *(NEC Laboratories Europe)*
- **Poster: SDN-based System to Filter Out DRDoS Amplification Traffic in ISP Networks** 2645
  Priyanka Dodia *(Qatar Computing Research Institute, HBKU)*, Yury Zhauniarovich *(Perfect Equanimity)*
- **Poster: GRANDPA Finality Gadget** 2649
  Alistair Stewart *(Web3 Foundation)*
- **Poster: Towards Characterizing and Limiting Information Exposure in DNN Layers** 2653
  Fan Mo *(Imperial College London)*, Ali Shahin Shamsabadi *(Queen Mary University of London)*,
  Kleomenis Katevas *(Imperial College London)*, Andrea Cavallaro *(Queen Mary University of London)*,
  Hamed Haddadi *(Imperial College London)*
- **Poster: Recovering the Input of Neural Networks via Single Shot Side-channel Attacks** 2657
  Lejla Batina *(Radboud University)*,
  Shivam Bhasin, Dirmanto Jap *(Nanyang Technological University, Singapore)*,
  Stjepan Picek *(Delft University of Technology)*
- **Poster: Challenges of Accurately Measuring Churn in P2P Botnets** 2661
  Leon Böck *(Technische Universität Darmstadt)*,
  Shankar Karuppayah *(Technische Universität Darmstadt & Universiti Sains Malaysia)*,
  Kory Fong *(RBC Research Institute)*, Max Mühlhäuser *(Technische Universität Darmstadt)*,
  Emmanouil Vasilomanolakis *(Aalborg University)*

- **Poster: TCLP: Enforcing Least Privileges to Prevent Containers from Kernel Vulnerabilities** 2665
Suyeol Lee, Junsik Seo, Jaehyun Nam, Seungwon Shin *(Korea Advanced Institute of Science and Technology)*
- **Poster: Let History not Repeat Itself (this Time) – Tackling WebAuthn Developer Issues Early On** 2669
Aftab Alam *(Saarland University)*,
Katharina Krombholz, Sven Bugiel *(CISPA Helmholtz Center for Information Security)*
- **Poster: When Adversary Becomes the Guardian– Towards Side-channel Security With Adversarial Attacks** 2673
Stjepan Picek *(Delft University of Technology)*,
Dirmanto Jap, Shivam Bhasin *(Nanyang Technological University)*
- **Poster: Towards Automated Quantitative Analysis and Forecasting of Vulnerability Discoveries in Debian GNU/Linux** 2677
Nikolaos Alexopoulos, Rolf Egert, Tim Grube, Max Mühlhäuser *(Technische Universität Darmstadt)*
- **Poster: Effective Layers in Coverage Metrics for Deep Neural Networks** 2681
Leo Hyun Park, Sangjin Oh, Jaeuk Kim, Soochang Chung, Taekyoung Kwon *(Yonsei University)*
- **Poster: Detecting WebAssembly-based Cryptocurrency Mining** 2685
Weikang Bian, Wei Meng *(Chinese University of Hong Kong)*,
Yi Wang *(Southern University of Science and Technology)*
- **Poster: Evaluating Code Coverage for System Call Fuzzers** 2689
Seoyoung Kim, Seyeon Jeong, Mingi Cho, Soochang Chung, Taekyoung Kwon *(Yonsei University)*

Workshop Summaries

- **CCSW'19 Workshop Summary – 2019 Cloud Computing Security Workshop** 2693
Radu Sion *(Stony Brook University)*, Charalampos Papamanthou *(University of Maryland)*
- **CPS-SPC 2019: Fifth Workshop on Cyber-Physical Systems Security and PrivaCy** 2695
Nils Ole Tippenhauer *(CISPA Helmholtz Center for Information Security)*,
Avishai Wool *(Tel Aviv University)*
- **MTD 2019: The 6th ACM Workshop on Moving Target Defense** 2697
Zhuo Lu *(University of South Florida)*
- **SSR'19: The 5th Conference on Security Standardisation Research** 2699
Maryam Mehrnezhad *(Newcastle University)*, Thyla van der Merwe *(Mozilla)*,
Feng Hao *(University of Warwick)*
- **TIS'19: Theory of Implementation Security Workshop 2019** 2701
Begül Bilgin *(Rambus-Cryptography Research)*, Svetla Nikova, Vincent Rijmen *(KU Leuven)*
- **WAHC'19: 7th Workshop on Encrypted Computing & Applied Homomorphic Cryptograph** 2703
Michael Brenner *(Leibniz Universität Hannover)*, Tancrède Lepoint *(Google)*,
Kurt Rohloff *(New Jersey Institute of Technology and Duality Technologies)*
- **18th Workshop on Privacy in the Electronic Society (WPES 2019)** 2705
Josep Domingo-Ferrer *(Universitat Rovira i Virgili)*
- **AISec'19: 12th ACM Workshop on Artificial Intelligence and Security** 2707
Sadia Afroz *(University of California, Berkeley)*, Battista Biggio *(University of Cagliari)*,
Nicholas Carlini *(Google Brain)*, Yuval Elovici, Asaf Shabtai *(Ben-Gurion University of the Negev)*
- **ASHES 2019 — 3rd Workshop on Attacks and Solutions in Hardware Security** 2709
Chip Hong Chang *(NTU Singapore)*, Daniel E. Holcomb *(University of Massachusetts at Amherst)*,
Francesco Regazzoni *(University of Lugano)*, Ulrich Rührmair *(LMU Munich)*,
Patrick Schaumont *(Virginia Tech)*
- **1st Workshop on Cyber-Security Arms Race (CYSARM 2019)** 2711
Thanassis Giannetsos *(Technical University of Denmark)*,
Daniele Sgandurra *(Royal Holloway, University of London)*

- **IoT S&P 2019: 2nd Workshop on the Internet of Things Security and Privacy** 2713
  Peng Liu *(Penn State University)*, Yuqing Zhang *(University of Chinese Academy of Sciences, China)*
- **PLAS 2019 - ACM SIGSAC Workshop on Programming Languages and Analysis for Security** 2715
  Piotr Mardziel *(Carnegie Mellon University)*, Niki Vazou *(IMDEA Software Institute)*
- **PPML '19: Privacy Preserving Machine Learning** 2717
  Borja Balle *(DeepMind)*, Adrià Gascón *(Google)*, Olya Ohrimenko *(Microsoft Research)*, Mariana Raykova *(Google)*, Phillipp Schoppmmann *(Humboldt-Universität zu Berlin)*, Carmela Troncoso *(École Polytechnique Fédérale de Lausanne)*
- **3rd International Workshop on Software Protection (SPRO 2019)** 2719
  Paolo Falcarin *(University of East London)*, Michael MiZu Zunke *(Thales Group)*

Author Index 2721

CCS 2019 Conference Organization

General Chairs:	Lorenzo Cavallaro (King's College London, UK) Johannes Kinder (Bundeswehr University Munich, Germany)
Program Chairs:	XiaoFeng Wang (Indiana University, USA) Jonathan Katz (George Mason University, USA)
Workshops Chair:	Thorsten Holz (Ruhr-University Bochum, Germany)
Poster / Demo Chair:	Stefan Brunthaler (Bundeswehr University Munich, Germany)
Panel Chair:	Adam Doupé (Arizona State University, USA)
Publication Chairs:	Brendan Dolan-Gavitt (New York University, USA) Gianluca Stringhini (Boston University, USA)
Web Chair:	Swen Jacobs (CISPA Helmholtz Center for Information Security, Germany)
Publicity Chairs:	Emiliano De Cristofaro (University College London, UK) Mark Manulis (University of Surrey, UK) Mathias Payer (EPFL, Switzerland)
Sponsorship Chairs:	Nick Nikiforakis (Stony Brook University, USA) Andrew Paverd (Microsoft Research, UK)
Student Travel Grant Chairs:	Katharina Krombholz (CISPA Helmholtz Center for Information Security, Germany) Elissa Redmiles (University of Maryland, USA) Hassan Takabi (University of North Texas, USA)
Registration Chairs:	Jorge Blasco Alis (Royal Holloway University of London, UK) Daniele Sgandurra (Royal Holloway University of London, UK)
Local Arrangements Chair:	Mia Robertson
Volunteer Chair:	Dan O'Keeffe (Royal Holloway University of London, UK)
Program Committee:	Gail-Joon Ahn (Arizona State University) Sumayah Alrwais (King Saud University) Owen Arden (UC Santa Cruz) Adam Aviv (The George Washington University) Erman Ayday (Case Western Reserve University) Michael Backes (CISPA Helmholtz Center for Information Security) Raef Bassily (Ohio State University)

Program Committee (continued):

Gilles Barthe (MPI Security and Privacy and IMDEA Software Institute)
Lujo Bauer (CMU)
Mihir Bellare (UCSD)
Karthikeyan Bhargavan (INRIA)
Leyla Bilge (Symantec)
Vincent Bindschaedler (University of Florida)
Jeremiah Blocki (Purdue University)
Rakesh Bobba (Oregon State University)
Sven Bugiel (CISPA Helmholtz Center for Information Security)
Christian Cachin (IBM Research Zürich)
L. Jean Camp (Indiana University)
Yinzhi Cao (Johns Hopkins University)
Alvaro Cardenas (UC Santa Cruz)
David Cash (University of Chicago)
Haibo Chen (Shanghai Jiao Tong University)
Hao Chen (University of California, Davis)
Hao Chen (MIcrosoft Research)
Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences, China)
Shuo Chen (Microsoft Research)
Yan Chen (Northwestern University)
Yingying Chen (Rutgers University)
Omar Chowdhury (The University of Iowa)
Nicolas Christin (Carnegie Mellon University)
Weidong Cui (Microsoft Research)
Lucas Davi (University of Duisburg-Essen)
Lorenzo De Carli (Worcester Polytechnic Institute)
Emiliano De Cristofaro (UCL)
Soteris Demetriou (Imperial College London)
Wenrui Diao (Shandong University)
Adam Doupe (Arizona State University)
Haixin Duan (360 ESG Institute of Security Research; Institute for Network Science and Cyberspace, Tsinghua University)
Tudor Dumitras (Univ. Maryland)
Manuel Egele (Boston University)
Ittay Eyal (Technion, Israel)
Sascha Fahl (University of Hannover)
Kassem Fawaz (University of Wisconsin-Madison)
Dario Fiore (IMDEA Software Institute)
Marc Fischlin (TU Darmstadt)
Sara Foresti (Università degli Studi di Milano)
Michael Franz (University of California, Irvine, USA)
Xinyang Ge (Penn State)
Daniel Genkin (University of Michigan)
Rosario Gennaro (City College, CUNY)
Irene Giacomelli (Protocol Labs)
Neil Gong (Duke University)
Guofei Gu (Texas A&M)
Yong Guan (Iowa State University)

Program Committee (continued):

Carl Gunter (University of Illinois)
Weili Han (Fudan University)
Carmit Hazay (Bar-Ilan University)
Ryan Henry (University of Calgary)
Michael Hicks (University of Maryland)
Thorsten Holz (Ruhr-University Bochum)
Nick Hopper (University of Minnesota)
Amir Houmansadr (UMass Amherst)
Yan Huang (Indiana University)
Trent Jaeger (Penn State University)
Tibor Jager (Paderborn University)
Rob Jansen (U.S. Naval Research Laboratory)
Somesh Jha (University of Wisconsin)
Shouling Ji (Zhejiang University)
Yier Jin (University of Florida)
Brent ByungHoon Kang (KAIST)
Murat Kantarcioglu (University of Texas at Dallas)
Alexandros Kapravelos (North Carolina State University)
Aniket Kate (Purdue University)
Jonathan Katz (University of Maryland)
Aggelos Kiayias (University of Edinburgh)
Taesoo Kim (Georgia Institute of Technology)
Yongdae Kim (KAIST)
Engin Kirda (Northeastern University)
Ralf Kuesters (University of Stuttgart, Germany)
Bum Jun Kwon (National Security Research Institute)
Ruby Lee (Princeton)
Wenke Lee (Georgia Institute of Technology)
Kirill Levchenko (University of Illinois Urbana-Champaign)
Bo Li (UIUC)
Ninghui Li (Purdue University)
Zhou Li (UC Irvine)
Zhenkai Liang (National University of Singapore)
Xiaojing Liao (Indiana University)
David Lie (Univ. Toronto)
Zhiqiang Lin (Ohio State University)
Peng Liu (Pennsylvania State University)
Yang Liu (Nanyang Technological University)
Wenjing Lou (Virginia Polytechnic Institute and State University)
Kangjie Lu (University of Minnesota)
Vadim Lyubashevsky (IBM Research - Zurich)
Ashwin Machanavajjhala (Duke University)
Matteo Maffei (TU Wien)
Mohammad Mannan (Concordia University)
Damon McCoy (NYU)
Patrick McDaniel (Penn State University)
Ian Miers (Cornell Tech; University of Maryland)
Andrew Miller (University of Illinois at Urbana-Champaign)
Jiang Ming (University of Texas at Arlington)

Program Committee (continued):

Ilya Mironov (Google)
Esfandiar Mohammadi (ETH Zurich)
Payman Mohassel (Yahoo Inc)
Muhammad Naveed (USC)
Stefan Nuernberger (CISPA Helmholtz Center i.G.)
Olya Ohrimenko (Microsoft Research)
Claudio Orlandi (Aarhus University)
Nicolas Papernot (Penn State)
Kenny Paterson (RHUL/ETH Zurich)
Mathias Payer (EPFL)
Paul Pearce (Georgia Tech; Facebook; International Computer Science Institute)
Adrian Perrig (ETH)
Frank Piessens (KU Leuven)
Feng Qian (University of Minnesota - Twin Cities)
Zhiyun Qian (UC Riverside)
Mike Reiter (UNC)
William Robertson (Northeastern University)
Mike Rosulek (Oregon State University)
Andrew Ruef (Independent)
Ulrich Rührmair (LMU Munich)
Andrei Sabelfeld (Chalmers University of Technology)
Ahmad-Reza Sadeghi (TU Darmstadt)
Nitesh Saxena (The University of Alabama at Birmingham)
Joshua Schiffman (HP Labs, HP Inc.)
Benedikt Schmidt (Google)
Dominique Schröder (Friedrich-Alexander Universität Erlangen-Nürnberg)
Abhi Shelat (Northeastern University)
Seungwon Shin (KAIST)
Reza Shokri (National University of Singapore (NUS))
Radu Sion (Stony Brook University)
Adam Smith (Boston University)
Chengyu Song (UC Riverside)
Ben Stock (CISPA Helmholtz Center for Information Security)
Gianluca Stringhini (Boston University)
Kun Sun (George Mason University)
Paul Syverson (U.S. Naval Research Laboratory)
Kunal Talwar (Google Inc)
Yuan Tian (University of Virginia)
Nils Ole Tippenhauer (CISPA Helmholtz-Zentrum i.G.)
Mohit Tiwari (University of Texas - Austin)
Blase Ur (University of Chicago)
Venkat Venkatakrishnan (UIC)
Giovanni Vigna (UC Santa Barbara)
Hayawardh Vijayakumar (Samsung Research America)
Haining Wang (University of Delaware)
Ruoyu "Fish" Wang (Arizona State University)
Wenhao Wang (Institute of Information Engineering, CAS)
XiaoFeng Wang (Indiana University Bloomington)

Program Committee (continued):

Xiao Wang (MIT, Boston University)
Rebecca Wright (Rutgers University)
Dinghao Wu (Pennsylvania State University)
Tao Xie (UIUC)
Luyi Xing (Indiana University Bloomington)
Xinyu Xing (Pennsylvania State University)
Li Xiong (Emory U)
Wenyuan Xu (Zhejiang University)
Min Yang (Fudan University)
Danfeng Yao (Virginia Tech, Dept of Computer Science)
Yuval Yarom (University of Adelaide and Data61)
Arkady Yerukhimovich (George Washington University)
Heng Yin (UC Riverside)
Ting Yu (Qatar Computing Research Institute)
Yu Yu (Shanghai Jiao Tong University)
Chao Zhang (Institute for Network Sciences and Cyberspace of Tsinghua University)
Danfeng Zhang (Penn State University)
Fengwei Zhang (Wayne State University)
Kehuan Zhang (The Chinese University of Hong Kong)
Xiangyu Zhang (Purdue University)
Yang Zhang (CISPA Helmholtz Center for Information Security)
Yinqian Zhang (Ohio State)
Yupeng Zhang (UC Berkeley)
Jianying Zhou (Singapore University of Technology and Design)
Yajin Zhou (Zhejiang University)
Zhe Zhou (Fudan University)

Additional reviewers:

Aydin Abadi
Shashank Agrawal
Seyed Mohammad Mehdi Ahmadpanah
Chuadhry Mujeeb Ahmed
Hasan Faik Alan
Arwa Alrawais
Vivek Arte
Enrico Bacis
Christian Badertscher
Shi Bai
Subarno Banerjee
Manuel Barbosa
Iulia Bastys
Fabrice Benhamouda
Jan Bobolz
Jonathan Bootle
Raphael Bost
Robert Brotzman
Carlo Brunetta
Jo Van Bulck
Quinn Burke
Andrei Bytes
Matteo Campanelli
Jiahao Cao
Yang Cao
Xavier de Carné de Carnavalet
Dario Catalano
Berkay Celik
Pyrros Chaidos
Hongyan Chang
Bo Chen
Hongxu Chen
Jianjun Chen

Additional reviewers (continued):

Jiongyi Chen
Joann Chen
Lingwei Chen
Sen Chen
Yang Chen
Yilei Chen
Chris Chao-Chun Cheng
Haehyun Cho
Michele Ciampi
Sandro Coretti-Drayton
Adrien Cosson
Wei Dai
Gareth Davies
Hannah Davis
Jiangyi Deng
Zeyu Ding
Shuaike Dong
Xiaoning Du
Benjamin Eriksson
Antonio Faonio
David Freeman
Chaya Ganesh
Xing Gao
Essam Ghadafi
Esha Ghosh
Neline van Ginkel
Huijing Gong
Benjamin Gregoire
Jinyu Gu
Xiaolan Gu
Le Guan
Chun Guo
HyungSeok Han
Yufei Han
Daniel Hedin
Andrew Hirsch
Grant Ho
Kyle Hogan
Pedram Hosseyni
Kaiyu Hou
Hongxin Hu
Remy Husson
Yongho Hwang
Joseph Jaeger
Xiangkun Jia
Yufei Jiang
Chenglu Jin
Lin Jin
Aaron Johnson
Chiraag Juvekar
Amir-Hossein Karimi
Mohammad Kavousi
Junming Ke
Miran Kim
Kamil Kluczniak
Dimitris Kolonelos
Karel Kubicek
Rafael Kurek
Russell W. F. Lai
Thalia Laing
Jonathan Lee
Anja Lehmann
Nikos Leonardos
Frank Li
Wenting Li
Xiaoting Li
Yanjie Li
Yuekang Li
Zengpeng Li
Zhenyuan Li
Julian Liedtke
Baojun Liu
Songsong Liu
Xiao Liu
Xueqing Liu
Jian Lou
Wouter Lueks
Shuaicheng Ma
Zeyu Mi
Peihan Miao
Mohsen Minaei
Pedro Moreno-Sanchez
Jan Tobias Muehlberg
Sasi Kumar Murakonda
Johannes Müller
Mohamed Nabeel
Yuhong Nan
Gregory Neven
Ruth Ng
Ngoc Khanh Nguyen
David Niehues
Jianting Ning
Luca Nizzardo
David Paaßen
Elena Pagnin
Eric Pauley
Gerardo Pelosi
Krzysztof Pietrzak

Additional reviewers (continued):

Rupesh Prajapati
Jay Prakash
Anais Querol
Ananth Raghunathan
Daniel Rausch
Peter Rindal
Michael Rodler
Viktoria Ronge
Carlos Rubio
Tim Ruffing
David Rupprecht
Leonid Ryzhyk
Ralf Sasse
Patrick Schaumont
Thomas Schneider
Jonas Schneider-Bensch
Andre Schrottenloher
Mahmood Sharif
Vishal Sharma
Ryan Sheatsley
Chen Shi
Junbum Shin
Mike Simon
David Sommer
Yongsoo Song
Igors Stepanovs
Aikaterini-Panagiota Stouka
Raoul Strackx
Haipei Sun
Jianhua Sun
Menghan Sun
Sebastian Surminski
Di Tang
Stefano Tessaro
Om Thakkar
Abhradeep Guha Thakurta
Sri Aravinda Krishnan Thyagarajan
Ni Trieu
Christine Utz
Kobe Vrancken
Shengye Wan
Li Wang
Pei Wang
Shu Wang
Xinda Wang
Yuxin Wang
Zihao Wang
Gaven Watson
Gaëtan Wattiau
Yibo Wu
Tim Würtele
Jidong Xiao
Yang Xiao
Yonghui Xiao
Xiaofei Xie
Chunlin Xiong
Fenghao Xu
Chen Yan
Wei Yang
Zheng Yang
Qingqing Ye
Yang Yu
Thomas Zacharias
Bin Zhang
Guomin Zhang
Jinquan Zhang
Ning Zhang
Qiuchen Zhang
Xian Zhang
Yubao Zhang
Yushi Zhang
Lianying Zhao
Ziming Zhao
Zirui Zhao
Ruiyu Zhu
Dionysis Zindros

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

Steering Committee:

David Basin (ETH Zurich)
Trent Jaeger (Pennsylvania State University)
Carl Landwehr (George Washington University)
Stefan Savage (University of California-San Diego)
Rebecca Wright (Rutgers University)

ACM CCS 2019 Sponsors & Supporters

Sponsor:

acm SIGSAC

Platinum Supporters:

facebook

intel®

NSF

Gold Supporters:

蚂蚁金服 ANT FINANCIAL

CISCO

Google

HUAWEI

جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

Microsoft

SAMSUNG
Research

Silver Supporters:

IBM Research

THE BEST RUN SAP

Bronze Supporters:

CLOUDFLARE

nccgroup

PlatON

TOSHIBA