

October 30–November 3, 2017
Dallas, TX, USA



Association for
Computing Machinery

Advancing Computing as a Science & Profession



CCS'17

Proceedings of the 2017 ACM SIGSAC Conference on
Computer and Communications Security

Sponsored by:

ACM SIGSAC



**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 © 2017 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: 978-1-4503-4946-8

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.

ACM CCS 2017 General Chair's Welcome

It is our great pleasure to welcome you to the 2017 ACM Conference on Computer and Communications Security (CCS) in Dallas, Texas. We are honored to organize ACM CCS 2017 in Dallas this year and extend our welcome to attendees from around the globe to this exciting city. We hope that you enjoy what the conference has to offer this year, both for the scientific discussions, and for the social events.

Dallas is one of the fastest growing urban area in America, with one million residents coming to the region every seven years. It is also one of the most demographically diverse and young cities in the country, which imbues the city with a friendly, outgoing sense of hospitality and genuine civic pride. Here you will find a large collection of international corporations, nationally recognized sports teams, and world class shopping. The Dallas Arts District and the many parks and gardens throughout Dallas will provide you with opportunities to enjoy the local culture while you are here.

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

CCS 2017 would not have been possible without the help of numerous volunteers. We first want to thank all the authors who have submitted their work to CCS – without their commitment CCS 2017 would never have been possible. We also thank the program chairs, the program committee and the entire ACM organization and SIGSAC steering committee for their dedication and commitment. Special thanks go to Ms. Rhonda Walls and her team for the wonderful handling of the organization. Last but not least, we would like to express our gratitude to our generous sponsors of the conference, listed in the program, for their valuable support.

We hope that you will find this program interesting and thought-provoking and that the conference will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world. We wish you a pleasant and enjoyable stay in Dallas, Texas.

Dr. Bhavani Thuraisingham

CCS 2017 General Chair

The University of Texas at Dallas

Richardson, Texas

Program Chairs' Welcome

Welcome to the 24th ACM Conference on Computer and Communications Security!

Since 1993, CCS has been the ACM's flagship conference for research in all aspects of computing and communications security and privacy. This year's conference attracted a record number of 836 reviewed research paper submissions, of which a record number of 151 papers were selected for presentation at the conference and inclusion in the proceedings.

The papers were reviewed by a Program Committee of 146 leading researchers from academic, government, and industry from around the world. Reviewing was done in three rounds, with every paper being reviewed by two PC members in the first round, and additional reviews being assigned in later rounds depending on the initial reviews. Authors had an opportunity to respond to reviews received in the first two rounds. We used a subset of PC members, designated as the Discussion Committee, to help ensure that reviewers reconsidered their reviews in light of the author responses and to facilitate substantive discussions among the reviewers. Papers were discussed extensively on-line in the final weeks of the review process, and late reviews were requested from both PC members and external reviewers when additional expertise or perspective was needed to reach a decision. We are extremely grateful to the PC members for all their hard work in the review process, and to the external reviewers that contributed to selecting the papers for CCS.

Before starting the review process, of the 842 submissions the PC chairs removed six papers that clearly violated submission requirements or were duplicates, leaving 836 papers to review. In general, we were lenient on the requirements, only excluding papers that appeared to deliberately disregard the submission requirements. Instead of excluding papers which carelessly deanonymized the authors, or which abused appendices in the opinion of the chairs, we redacted (by modifying the submitted PDF) the offending content and allowed the papers to be reviewed, and offered to make redacted content in appendices available to reviewers upon request.

Our review process involved three phases. In the first phase, each paper was assigned two reviewers. Following last year's practice, we adopted the Toronto Paper Matching System (TPMS) for making most of the review assignments, which were then adjusted based on technical preferences declared by reviewers. Each reviewer had about 3 weeks to complete reviews for around 12 papers. Based on the results of these reviews, an additional reviewer was assigned to every paper that had at least one positive-leaning review. Papers where both initial reviews were negative, but with low confidence or significant positive aspects, were also assigned additional reviews. At the conclusion of the second reviewing round, authors had an opportunity to see the initial reviews and to submit a short rebuttal. To ensure that all the authors' responses were considered seriously by the reviewers, the Discussion Committee members worked closely with the reviewers to make sure that they considered and responded to the authors' rebuttals. When reviewers could not reach an agreement, or additional expertise was needed, we solicited additional reviews. The on-line discussion period was vibrant and substantive, and at the end of this process the 151 papers you find here were selected for CCS 2017.

We are grateful to all the PC members and external reviewers for their hard work and thoughtful discussions; to the General Chair, Bhavani Thuraisingham, for saving us from having to deal with anything other than the program and answering all our questions promptly and helpfully; to the Proceedings Chairs, Matthew Wright and Apu Kapadia, for all their efforts working with the

publisher to produce the proceedings; to Hui Lu for managing the submission server and its interface with TPMS; and to all the authors who submitted papers to CCS.

We hope everyone finds the conference engaging, enlightening, and inspiring!

David Evans

University of Virginia

Tal Maklin

Columbia University

Dongyan Xu

Purdue University

ACM CCS 2017 Program Committee Co-Chairs

Table of Contents

CCS 2017 Conference Organization	xxii
--	------

Keynote Talk

- **Security and Machine Learning** 1
David Wagner (*University of California, Berkeley*)

Session A1: Multi-Party Computation 1

- **DUPLO: Unifying Cut-and-Choose for Garbled Circuits** 3
Vladimir Kolesnikov (*Bell Labs*), Jesper Buus Nielsen, Mike Rosulek, Ni Trieu (*Oregon State University*), Roberto Trifiletti (*Aarhus University*)
- **Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation**..... 21
Xiao Wang (*University of Maryland*), Samuel Ranellucci (*University of Maryland & George Mason University*), Jonathan Katz (*University of Maryland*),
- **Global-Scale Secure Multiparty Computation**..... 39
Xiao Wang (*University of Maryland*), Samuel Ranellucci (*University of Maryland & George Mason University*), Jonathan Katz (*University of Maryland*)

Session A2: Human Authentication

- **Hearing Your Voice is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication** 57
Linghan Zhang, Sheng Tan, Jie Yang (*Florida State University*)
- **VibWrite: Towards Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration** 73
Jian Liu, Chen Wang, Yingying Chen (*Rutgers University*), Nitesh Saxena (*University of Alabama at Birmingham*)
- **Presence Attestation: The Missing Link in Dynamic Trust Bootstrapping** 89
Zhangkai Zhang (*Beihang University*), Xuhua Ding (*Singapore Management University*), Gene Tsudik (*University of California, Irvine*), Jinhua Cui (*Singapore Management University*), Zhoujun Li (*Beihang University*)

Session A3: Adversarial Machine Learning

- **DolphinAttack: Inaudible Voice Commands** 103
Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, Wenyan Xu (*Zhejiang University*)
- **Evading Classifiers by Morphing in the Dark** 119
Hung Dang, Yue Huang, Ee-Chien Chang (*National University of Singapore*)
- **MagNet: A Two-Pronged Defense against Adversarial Examples**..... 135
Dongyu Meng (*ShanghaiTech University*), Hao Chen (*University of California, Davis*)

Session A4: Browsers

- **Hindsight: Understanding the Evolution of UI Vulnerabilities in Mobile Browsers** 149
Meng Luo, Oleksii Starov, Nima Honarmand, Nick Nikiforakis (*Stony Brook University*)
- **Deterministic Browser** 163
Yinzhao Cao, Zhanhao Chen, Song Li, Shujiang Wu (*Lehigh University*)
- **Most Websites Don't Need to Vibrate: A Cost-Benefit Approach to Improving Browser Security** 179
Peter Snyder, Cynthia Taylor, Chris Kanich (*University of Illinois at Chicago*)

Session A5: Cryptocurrency

- **Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin** 195
Yujin Kwon, Dohyun Kim, Yunmok Son (*Korea Advanced Institute of Science and Technology*),
Eugene Vasserman (*Kansas State University*), Yongdae Kim (*Korea Advanced Institute of Science and Technology*)
- **Betrayal, Distrust, and Rationality: Smart Counter-Collusion Contracts for Verifiable Cloud Computing** 211
Changyu Dong, Yilei Wang, Amjad Aldweesh (*Newcastle University*),
Patrick McCorry (*University College London*), Aad van Moorsel (*Newcastle University*)
- **Zero-Knowledge Contingent Payments Revisited: Attacks and Payments for Services** 229
Matteo Campanelli (*City University of New York Graduate Center*),
Rosario Gennaro (*City College of New York*), Steven Goldfeder (*Princeton University*),
Luca Nizzardo (*IMDEA Software Institute & Universidad Politécnica de Madrid*)

Session B1: Multi-Party Computation 2

- **Pool: Scalable On-Demand Secure Computation Service Against Malicious Adversaries** 245
Ruiyu Zhu, Yan Huang (*Indiana University*), Darion Cassel (*Carnegie Mellon University & Indiana University*)
- **A Framework for Constructing Fast MPC over Arithmetic Circuits with Malicious Adversaries and an Honest-Majority** 259
Yehuda Lindell, Ariel Nof (*Bar-Ilan University*)
- **Efficient, Constant-Round and Actively Secure MPC: Beyond the Three-Party Case** 277
Nishanth Chandran (*Microsoft Research India*), Juan A. Garay (*Texas A&M University & Yahoo Research*),
Payman Mohassel (*Visa Research*), Satyanarayana Vusirikala (*Microsoft Research India*)

Session B2: Passwords

- **Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat** 295
Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin,
Lorrie Faith Cranor (*Carnegie Mellon University*), Serge Egelman (*International Computer Science Institute*),
Alain Forget (*Google, Inc.*)
- **Why Do Developers Get Password Storage Wrong? A Qualitative Usability Study** 311
Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand,
Matthew Smith (*University of Bonn*)
- **The TypTop System: Personalized Typo-Tolerant Password Checking** 329
Rahul Chatterjee (*Cornell University & Cornell Tech*), Joanne Woodage (*Royal Holloway, University of London*),
Yuval Pnueli (*Technion – Israel Institute of Technology*), Anusha Chowdhury (*Cornell University*),
Thomas Ristenpart (*Cornell University & Cornell Tech*)

Session B3: Investigating Attacks

- **Rise of the HaCRS: Augmenting Autonomous Cyber Reasoning Systems with Human Assistance** 347
Yan Shoshitaishvili (*Arizona State University*), Michael Weissbacher (*Northeastern University*),
Lukas Dresel, Christopher Salls, Ruoyu Wang, Christopher Kruegel,
Giovanni Vigna (*University of California, Santa Barbara*)
- **Neural Network-based Graph Embedding for Cross-Platform Binary Code Similarity Detection** 363
Xiaojun Xu (*Shanghai Jiao Tong University*), Chang Liu (*University of California, Berkeley*),
Qian Feng (*Samsung Research America*), Heng Yin (*University of California, Riverside*),
Le Song (*Georgia Institute of Technology*), Dawn Song (*University of California, Berkeley*)
- **RAIN: Refinable Attack Investigation with On-demand Inter-Process Information Flow Tracking** 377
Yang Ji, Sangho Lee, Evan Downing, Weiren Wang, Mattia Fazzini, Taesoo Kim, Alessandro Orso,
Wenke Lee (*Georgia Institute of Technology*)

Session B4: Privacy Policies

- **Synthesis of Probabilistic Privacy Enforcement** 391
Martin Kučera, Petar Tsankov, Timon Gehr, Marco Guarnieri, Martin Vechev (*ETH Zurich*)
- **A Type System for Privacy Properties** 409
Véronique Cortier (*CNRS, LORIA*), Niklas Grimm (*TU Wien*), Joseph Lallemand (*Inria, LORIA*), Matteo Maffei (*TU Wien*)
- **Generating Synthetic Decentralized Social Graphs with Local Differential Privacy** 425
Zhan Qin (*State University of New York at Buffalo & Hamad Bin Khalifa University*), Ting Yu, Yin Yang, Issa Khalil (*Hamad Bin Khalifa University*), Xiaokui Xiao (*Nanyang Technological University*), Kui Ren (*State University of New York at Buffalo & Qatar Computing Research Institute*)

Session B5: Blockchains

- **Revive: Rebalancing Off-Blockchain Payment Networks** 439
Rami Khalil, Arthur Gervais (*ETH Zurich*)
- **Concurrency and Privacy with Payment-Channel Networks** 455
Giulio Malavolta (*Friedrich-Alexander-University Erlangen-Nürnberg*), Pedro Moreno-Sanchez, Aniket Kate (*Purdue University*), Matteo Maffei (*TU Wien*), Srivatsan Ravi (*University of Southern California*)
- **Bolt: Anonymous Payment Channels for Decentralized Currencies**..... 473
Matthew Green, Ian Miers (*Johns Hopkins University*)

Session C1: Oblivious RAM

- **S3ORAM: A Computation-Efficient and Constant Client Bandwidth Blowup ORAM with Shamir Secret Sharing** 491
Thang Hoang, Ceyhan D. Ozkaptan, Attila A. Yavuz (*Oregon State University*), Jorge Guajardo (*Robert Bosch RTC*), Tam Nguyen (*Oregon State University*)
- **Deterministic, Stash-Free Write-Only ORAM** 507
Daniel S. Roche, Adam Aviv, Seung Geol Choi, Travis Mayberry (*United States Naval Academy*)
- **Scaling ORAM for Secure Computation** 523
Jack Doerner, Abhi Shelat (*Northeastern University*)

Session C2: World Wide Web of Wickedness

- **Don't Let One Rotten Apple Spoil the Whole Barrel: Towards Automated Detection of Shadowed Domains** 537
Daiping Liu (*University of Delaware*), Zhou Li (*ACM Member*), Kun Du (*Tsinghua University*), Haining Wang (*University of Delaware*), Baojun Liu, Haixin Duan (*Tsinghua University*)
- **Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting** 553
Samaneh Tajalizadehkhoob (*Delft University of Technology*), Tom Van Goethem (*imec-DistriNet, KU Leuven*), Maciej Korczyński, Arman Noroozian (*Delft University of Technology*), Rainer Böhme (*Innsbruck University*), Tyler Moore (*University of Tulsa*), Wouter Joosen (*imec-DistriNet, KU Leuven*), Michel van Eeten (*Delft University of Technology*)
- **Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse** 569
Panagiotis Kintis (*Georgia Institute of Technology*), Najmeh Miramirkhani (*Stony Brook University*), Charles Lever, Yizheng Chen, Rosa Romero-Gómez (*Georgia Institute of Technology*), Nikolaos Pitropakis (*London South Bank University*), Nick Nikiforakis (*Stony Brook University*), Manos Antonakakis (*Georgia Institute of Technology*)

Session C3: Machine Learning Privacy

- **Machine Learning Models that Remember Too Much** 587
Congzheng Song (*Cornell University*), Thomas Ristenpart, Vitaly Shmatikov (*Cornell Tech*)
- **Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning** 603
Briland Hitaj (*Stevens Institute of Technology & University of Rome - La Sapienza*),
Giuseppe Ateniese, Fernando Perez-Cruz (*Stevens Institute of Technology*)
- **Oblivious Neural Network Predictions via MiniONN Transformations** 619
Jian Liu, Mika Juuti, Yao Lu, N. Asokan (*Aalto University*)

Session C4: From Verification to ABE

- **Verifying Security Policies in Multi-agent Workflows with Loops** 633
Bernd Finkbeiner (*CISPA, Saarland University*),
Christian Müller, Helmut Seidl, Eugen Zălinescu (*Technische Universität München*)
- **Attribute-Based Encryption in the Generic Group Model: Automated Proofs and New Constructions** 647
Miguel Ambrona (*IMDEA Software Institute & Universidad Politecnica de Madrid*),
Gilles Barthe (*IMDEA Software Institute*), Romain Gay (*ENS*), Hoeteck Wee (*CNRS & ENS*)
- **FAME: Fast Attribute-based Message Encryption** 665
Shashank Agrawal (*Visa Research & Microsoft Research*), Melissa Chase (*Microsoft Research*)

Session C5: Using Blockchains

- **Practical UC-Secure Delegatable Credentials with Attributes and Their Application to Blockchain** 683
Jan Camenisch (*IBM Research - Zurich*), Manu Drijvers (*IBM Research - Zurich & ETH Zurich*),
Maria Dubovitskaya (*IBM Research - Zurich*)
- **Solidus: Confidential Distributed Ledger Transactions via PVORM** 701
Ethan Cecchetti, Fan Zhang, Yan Ji (*Cornell University; IC3*), Ahmed Kosba (*University of Maryland; IC3*),
Ari Juels (*Cornell Tech, Jacobs Institute; IC3*), Elaine Shi (*Cornell University; IC3*)
- **Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards** 719
Arka Rai Choudhuri, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, Ian Miers
(*Johns Hopkins University*)

Session D1: Functional Encryption and Obfuscation

- **5Gen-C: Multi-input Functional Encryption and Program Obfuscation for Arithmetic Circuits** 747
Brent Carmer (*Oregon State University & Galois, Inc.*), Alex J. Malozemoff (*Galois, Inc.*),
Mariana Raykova (*Yale University*)
- **IRON: Functional Encryption using Intel SGX** 765
Ben Fisch (*Stanford University*), Dhinakaran Vinayagamurthy (*University of Waterloo*),
Dan Boneh (*Stanford University*), Sergey Gorbunov (*University of Waterloo*)
- **Implementing BP-Obfuscation Using Graph-Induced Encoding** 783
Shai Halevi (*IBM Research*), Tzipora Halevi (*CUNY Brooklyn College*),
Victor Shoup (*IBM Research & New York University*),
Noah Stephens-Davidowitz (*New York University*)

Session D2: Vulnerable Mobile Apps

- **AUTHSCOPE: Towards Automatic Discovery of Vulnerable Authorizations in Online Services** 799
Chaoshun Zuo, Qingchuan Zhao, Zhiqiang Lin (*University of Texas at Dallas*)

- **Mass Discovery of Android Traffic Imprints through Instantiated Partial Execution** 815
Yi Chen (*Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences*), Wei You, Yeonjoon Lee (*Indiana University, Bloomington*), Kai Chen (*Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences*), XiaoFeng Wang (*Indiana University, Bloomington*), Wei Zou (*Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences*)
- **Unleashing the Walking Dead: Understanding Cross-App Remote Infections on Mobile WebViews** 829
Tongxin Li (*Peking University & Indiana University, Bloomington*), Xueqiang Wang (*Indiana University, Bloomington*), Mingming Zha, Kai Chen (*Institute of Information Engineering & Chinese Academy of Sciences & University of Chinese Academy of Sciences*), XiaoFeng Wang, Luyi Xing (*Indiana University, Bloomington*), Xiaolong Bai (*Tsinghua University*), Nan Zhang (*Indiana University, Bloomington*), Xinhui Han (*Peking University*)

Session D3: Logical Side Channels

- **May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519**..... 845
Daniel Genkin (*University of Pennsylvania & University of Maryland*), Luke Valenta (*University of Pennsylvania*), Yuval Yarom (*University of Adelaide & Data61*)
- **STACCO: Differentially Analyzing Side-Channel Traces for Detecting SSL/TLS Vulnerabilities in Secure Enclaves**..... 859
Yuan Xiao, Mengyuan Li, Sanchuan Chen, Yinqian Zhang (*Ohio State University*)
- **Precise Detection of Side-Channel Vulnerabilities using Quantitative Cartesian Hoare Logic** 875
Jia Chen, Yu Feng, Isil Dillig (*University of Texas at Austin*)

Session D4: Crypto Primitives

- **Better Than Advertised: Improved Collision-Resistance Guarantees for MD-Based Hash Functions** 891
Mihir Bellare, Joseph Jaeger, Julia Len (*University of California, San Diego*)
- **Generic Semantic Security against a Kleptographic Adversary** 907
Alexander Russell (*University of Connecticut*), Qiang Tang (*New Jersey Institute of Technology*), Moti Yung (*Snap.Inc & Columbia University*), Hong-Sheng Zhou (*Virginia Commonwealth University*)
- **Defending Against Key Exfiltration: Efficiency Improvements for Big-Key Cryptography via Large-Alphabet Subkey Prediction** 923
Mihir Bellare, Wei Dai (*University of California, San Diego*)

Session D5: Network Security

- **Client-side Name Collision Vulnerability in the New gTLD Era: A Systematic Study** 941
Qi Alfred Chen (*University of Michigan*), Matthew Thomas, Eric Osterweil (*Verisign Labs*), Yulong Cao, Jie You, Z. Morley Mao (*University of Michigan*)
- **The Wolf of Name Street: Hijacking Domains Through Their Nameservers**..... 957
Thomas Vissers (*imec-DistriNet, KU Leuven*), Timothy Barron (*Stony Brook University*), Tom Van Goethem, Wouter Joosen (*imec-DistriNet, KU Leuven*), Nick Nikiforakis (*Stony Brook University*)
- **Faulds: A Non-Parametric Iterative Classifier for Internet-Wide OS Fingerprinting**..... 971
Zain Shamsi, Daren B.H. Cline, Dmitri Loguinov (*Texas A&M University*)

Session E1: Hardening Crypto

- **T/Key: Second-Factor Authentication From Secure Hash Chains** 983
Dmitry Kogan, Nathan Manohar, Dan Boneh (*Stanford University*)

- **Practical Graphs for Optimal Side-Channel Resistant Memory-Hard Functions** 1001
Joel Alwen (*IST Austria*), Jeremiah Blocki, Ben Harsha (*Purdue University*)
- **Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation** 1019
Shay Gueron (*University of Haifa and Amazon Web Services*), Yehuda Lindell (*Bar-Ilan University*)

Session E2: Securing Mobile Apps

- **The ART of App Compartmentalization: Compiler-based Library Privilege Separation on Stock Android** 1037
Jie Huang, Oliver Schranz, Sven Bugiel, Michael Backes (*Saarland University*)
- **Vulnerable Implicit Service: A Revisit** 1051
Lingguang Lei (*Chinese Academy of Sciences & Institute of Information Engineering, Chinese Academy of Sciences*), Yi He (*Tsinghua University*), Kun Sun (*George Mason University*), Jiwu Jing, Yuewu Wang (*Chinese Academy of Sciences & Institute of Information Engineering, Chinese Academy of Sciences*), Qi Li (*Tsinghua University*), Jian Weng (*Jinan University*)
- **A Stitch in Time: Supporting Android Developers in Writing Secure Code** 1065
Duc Cuong Nguyen (*Saarland University*), Dominik Wermke, Yasemin Acar (*Leibniz University, Hannover*), Michael Backes (*Saarland University*), Charles Weir (*Lancaster University*), Sascha Fahl (*Leibniz University, Hannover*)

Session E3: Physical Side Channels

- **Exploiting a Thermal Side Channel for Power Attacks in Multi-Tenant Data Centers** 1079
Mohammad A. Islam, Shaolei Ren (*University of California, Riverside*), Adam Wierman (*California Institute of Technology*)
- **Watch Me, but Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations** 1095
Yi Han, Sriharsha Etigowni, Hua Liu, Saman Zonouz, Athina Petropulu (*Rutgers University*)
- **Viden: Attacker Identification on In-Vehicle Networks** 1109
Kyong-Tak Cho, Kang G. Shin (*University of Michigan*)

Session E4: Adversarial Social Networking

- **Practical Attacks Against Graph-based Clustering** 1125
Yizheng Chen, Yacin Nadji, Athanasios Kountouras (*Georgia Institute of Technology*), Fabian Monroe (*University of North Carolina at Chapel Hill*), Roberto Perdisci (*University of Georgia*), Manos Antonakakis (*Georgia Institute of Technology*), Nikolaos Vasiloglou (*Symantec CAML Group*)
- **Automated Crowdturfing Attacks and Defenses in Online Review Systems** 1143
Yuanshun Yao, Bimal Viswanath, Jenna Cryan, Haitao Zheng, Ben Y. Zhao (*University of Chicago*)
- **POISED: Spotting Twitter Spam Off the Beaten Paths** 1159
Shirin Nilizadeh (*University of California, Santa Barbara*), Francois Labrèche, Alireza Sedighian (*Ecole Polytechnique de Montréal*), Ali Zand (*University of California, Santa Barbara*), José Fernandez (*Ecole Polytechnique de Montréal*), Christopher Kruegel (*University of California, Santa Barbara*), Gianluca Stringhini (*University College London*), Giovanni Vigna (*University of California, Santa Barbara*)

Session E5: Privacy-Preserving Analytics

- **Practical Secure Aggregation for Privacy-Preserving Machine Learning** 1175
Keith Bonawitz, Vladimir Ivanov, Ben Kreuter (*Google Inc.*), Antonio Marcedone (*Cornell Tech*), H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, Karn Seth (*Google Inc.*)
- **Use Privacy in Data-Driven Systems: Theory and Experiments with Machine Learnt Programs** 1193
Anupam Datta, Matthew Fredrikson, Gihyuk Ko, Piotr Mardziel, Shayak Sen (*Carnegie Mellon University*)
- **SGX-BigMatrix: A Practical Encrypted Data Analytic Framework With Trusted Processors** 1211
Fahad Shaon, Murat Kantarcioglu, Zhiqiang Lin, Latifur Khan (*University of Texas at Dallas*)

Session F1: Private Set Intersection

- **Malicious-Secure Private Set Intersection via Dual Execution** 1229
Peter Rindal, Mike Rosulek (*Oregon State University*)
- **Fast Private Set Intersection from Homomorphic Encryption** 1243
Hao Chen, Kim Laine (*Microsoft Research*), Peter Rindal (*Oregon State University*)
- **Practical Multi-party Private Set Intersection from Symmetric-Key Techniques** 1257
Vladimir Kolesnikov (*Bell Labs*), Naor Matania, Benny Pinkas (*Bar-Ilan University*),
Mike Rosulek, Ni Trieu (*Oregon State University*)

Session F2: Insights from Log(in)s

- **Detecting Structurally Anomalous Logins Within Enterprise Networks** 1273
Hossein Siadati, Nasir Memon (*New York University*)
- **DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning** 1285
Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar (*University of Utah*)
- **RiskTeller: Predicting the Risk of Cyber Incidents** 1299
Leyla Bilge, Yufei Han, Matteo Dell'Amico (*Symantec Research Labs*)

Session F3: Crypto Pitfalls

- **Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2** 1313
Mathy Vanhoef, Frank Piessens (*imec-DistriNet, KU Leuven*)
- **CCCP: Closed Caption Crypto Phones to Resist MITM Attacks, Human Errors and Click-Through** 1329
Maliheh Shirvanian, Nitesh Saxena (*University of Alabama at Birmingham*)
- **No-Match Attacks and Robust Partnering Definitions – Defining Trivial Attacks for Security Protocols is Not Trivial** 1343
Yong Li (*Huawei Technologies Düsseldorf*), Sven Schäge (*Ruhr-Universität Bochum*)

Session F4: Private Queries

- **Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR** 1361
Syed Mahbub Hafiz, Ryan Henry (*Indiana University*)
- **PeGaSus: Data-Adaptive Differentially Private Stream Processing** 1375
Yan Chen, Ashwin Machanavajjhala (*Duke University*), Michael Hay (*Colgate University*),
Gerome Miklau (*University of Massachusetts, Amherst*)
- **Composing Differential Privacy and Secure Computation: A Case Study on Scaling Private Record Linkage** 1389
Xi He, Ashwin Machanavajjhala (*Duke University*), Cheryl Flynn, Divesh Srivastava (*AT&T Labs-Research*)

Session F5: Understanding Security Fails

- **Where the Wild Warnings Are: Root Causes of Chrome HTTPS Certificate Errors** 1407
Mustafa Emre Acer, Emily Stark, Adrienne Porter Felt (*Google Inc.*),
Sascha Fahl (*Leibniz University Hannover*), Radhika Bhargava (*Purdue University*),
Bhanu Dev (*International Institute of Information Technology, Hyderabad*),
Matt Braithwaite, Ryan Sleevi, Parisa Tabriz (*Google Inc.*)
- **Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials** 1421
Kurt Thomas (*Google*), Frank Li (*University of California, Berkeley*),
Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu,
Vijay Eranti, Angelika Moscicki, Daniel Margolis (*Google*),
Vern Paxson (*University of California, Berkeley & International Computer Science Institute*),
Elie Bursztein (*Google*)
- **Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI** 1435
Doowon Kim, Bum Jun Kwon, Tudor Dumitraş (*University of Maryland*)

Session G1: Searchable Encryption

- **Forward Secure Dynamic Searchable Symmetric Encryption with Efficient Updates** 1449
Kee Sung Kim, Minkyu Kim, Dongsoo Lee, Je Hong Park, Woo-Hwan Kim (*National Security Research Institute*)
- **Forward and Backward Private Searchable Encryption from Constrained Cryptographic Primitives** 1465
Raphaël Bost (*Direction Générale de l'Armement & Université de Rennes 1*),
Brice Minaud (*Royal Holloway, University of London*), Olga Ohrimenko (*Microsoft Research*)

Session G2: Bug-Hunting Risks and Rewards

- **Economic Factors of Vulnerability Trade and Exploitation** 1483
Luca Allodi (*Eindhoven University of Technology*)
- **Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research** 1501
Alexander Gamero-Garrido, Stefan Savage, Kirill Levchenko, Alex C. Snoeren
(*University of California, San Diego*)

Session G3: Crypto Standards

- **Identity-Based Format-Preserving Encryption** 1515
Mihir Bellare (*University of California, San Diego*), Viet Tung Hoang (*Florida State University*)
- **Standardizing Bad Cryptographic Practice: A Teardown of the IEEE Standard for Protecting Electronic-design Intellectual Property** 1533
Animesh Chhotaray, Adib Nahiyan, Thomas Shrimpton, Domenic Forte,
Mark Tehranipoor (*University of Florida*)

Session G4: Voting

- **New Techniques for Structural Batch Verification in Bilinear Groups with Applications to Groth-Sahai Proofs** 1547
Gottfried Herold (*Ecole Normale Supérieure*), Max Hoffmann (*Ruhr-Universität Bochum*),
Michael Klooß (*Karlsruhe Institute of Technology*), Carla Ràfols (*Universitat Pompeu Fabra*),
Andy Rupp (*Karlsruhe Institute of Technology*)
- **Practical Quantum-Safe Voting from Lattices** 1565
Rafaël del Pino, Vadim Lyubashevsky, Gregory Neven, Gregor Seiler (*IBM Research - Zurich*)

Session G5: Hardening Hardware

- **A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components ...** 1583
Vasilios Mavroudis, Andrea Cerulli (*University College London*), Petr Svenda (*Masaryk University*),
Dan Cvrcek, Dusan Klinec (*EnigmaBridge*), George Danezis (*University College London*)
- **Provably-Secure Logic Locking: From Theory To Practice** 1601
Muhammad Yasin (*New York University*), Abhrajit Sengupta (*New York University*),
Mohammed Thari Nabeel, Mohammed Ashraf (*New York University Abu Dhabi*),
Jeyavijayan (JV) Rajendran (*University of Texas at Dallas & Texas A&M University*),
Ozgur Sinanoglu (*New York University Abu Dhabi*)

Session H1: Crypto Attacks

- **The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli..** 1631
Matus Nemec (*Masaryk University, Ca' Foscari University of Venice*),
Marek Sys, Petr Svenda (*Masaryk University*), Dusan Klinec (*EnigmaBridge, Masaryk University*),
Vashek Matyas (*Masaryk University*)
- **Algorithm Substitution Attacks from a Steganographic Perspective** 1649
Sebastian Berndt, Maciej Liśkiewicz (*University of Lübeck*)
- **On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs ...** 1661
Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, Christian Boit (*Technische Universität Berlin*)

Session H2: Code Reuse Attacks

- **The Dynamics of Innocent Flesh on the Bone: Code Reuse Ten Years Later** 1675
Victor van der Veen, Dennis Andriesse, Manolis Stamatogiannakis (*Vrije Universiteit Amsterdam*),
Xi Chen (*Vrije Universiteit Amsterdam & Microsoft*),
Herbert Bos, Cristiano Giuffrida (*Vrije Universiteit Amsterdam*)
- **Capturing Malware Propagations with Code Injections and Code-Reuse Attacks** 1691
David Korczynski (*University of Oxford*), Heng Yin (*University of California, Riverside*)
- **Code-Reuse Attacks for the Web: Breaking Cross-Site Scripting Mitigations via Script Gadgets**..... 1709
Sebastian Lekies, Krzysztof Kotowicz (*Google*), Samuel Groß (*SAP*),
Eduardo A. Vela Nava (*Google*), Martin Johns (*SAP*)

Session H3: Web Security

- **Tail Attacks on Web Applications** 1725
Huasong Shan, Qingyang Wang (*Louisiana State University*), Calton Pu (*Georgia Institute of Technology*)
- **Rewriting History: Changing the Archived Web from the Present**..... 1741
Ada Lerner (*Wellesley College*), Tadayoshi Kohno, Franziska Roesner (*University of Washington*)
- **Deemon: Detecting CSRF with Dynamic Analysis and Property Graphs**..... 1757
Giancarlo Pellegrino (*CISPA, Saarland University*), Martin Johns (*SAP SE*),
Simon Koch, Michael Backes, Christian Rossow (*CISPA, Saarland University*)

Session H4: Formal Verification

- **A Comprehensive Symbolic Analysis of TLS 1.3** 1773
Cas Cremers (*University of Oxford*), Marko Horvat (*MPI-SWS*),
Jonathan Hoyland, Sam Scott, Thyla van der Merwe (*Royal Holloway, University of London*)
- **HACL*: A Verified Modern Cryptographic Library** 1789
Jean-Karim Zinzindohoué, Karthikeyan Bhargavan (*INRIA*), Jonathan Protzenko (*Microsoft Research*),
Benjamin Beurdouche (*INRIA*)
- **Jasmin: High-Assurance and High-Speed Cryptography** 1807
José Bacelar Almeida (*INESC TEC and Universidade do Minho*),
Manuel Barbosa (*INESC TEC and FCUP Universidade do Porto*), Gilles Barthe (*IMDEA Software Institute*),
Arthur Blot (*ENS Lyon*), Benjamin Grégoire (*Inria Sophia-Antipolis*), Vincent Laporte (*IMDEA Software Institute*),
Tiago Oliveira (*INESC TEC and FCUP Universidade do Porto*), Hugo Pacheco (*INESC TEC and Universidade do Minho*),
Benedikt Schmidt (*Google Inc.*), Pierre-Yves Strub (*École Polytechnique*)

Session I1: Post-Quantum

- **Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives**..... 1825
Melissa Chase (*Microsoft Research*), David Derler (*Graz University of Technology*),
Steven Goldfeder (*Princeton University*), Claudio Orlandi (*Aarhus University*),
Sebastian Ramacher (*Graz University of Technology*),
Christian Rechberger (*Graz University of Technology & Denmark Technical University*),
Daniel Slamanig (*AIT Austrian Institute of Technology*), Greg Zaverucha (*Microsoft Research*)
- **To BLISS-B or not to be - Attacking strongSwan's Implementation of Post-Quantum Signatures** 1843
Peter Pessl (*Graz University of Technology*), Leon Groot Bruinderink (*Technische Universiteit Eindhoven*),
Yuval Yarom (*University of Adelaide and Data61*)
- **Side-Channel Attacks on BLISS Lattice-Based Signatures: Exploiting Branch Tracing against strongSwan and Electromagnetic Emanations in Microcontrollers** 1857
Thomas Espitau (*UPMC*), Pierre-Alain Fouque (*Université de Rennes I*), Benoît Gérard (*DGA.MI*),
Mehdi Tibouchi (*NTT Corporation*)

Session I2: Information Flow

- **Nonmalleable Information Flow Control** 1875
Ethan Cecchetti, Andrew C. Myers (*Cornell University*),
Owen Arden (*University of California, Santa Cruz & Harvard University*)
- **Cryptographically Secure Information Flow Control on Key-Value Stores** 1893
Lucas Wayne, Pablo Buiras (*Harvard University*), Owen Arden (*University of California, Santa Cruz*),
Alejandro Russo (*Chalmers University of Technology*), Stephen Chong (*Harvard University*)
- **Object Flow Integrity** 1909
Wenhao Wang, Xiaoyang Xu, Kevin W. Hamlen (*University of Texas at Dallas*)

Session I3: Personal Privacy

- **BBA+: Improving the Security and Applicability of Privacy-Preserving Point Collection** 1925
Gunnar Hartung (*Karlsruhe Institute of Technology*), Max Hoffmann (*Ruhr-Universität Bochum*),
Matthias Nagel, Andy Rupp (*Karlsruhe Institute of Technology*)
- **walk2friends: Inferring Social Links from Mobility Profiles** 1943
Michael Backes (*Saarland University*), Mathias Humbert (*ETH Zurich and EPFL*),
Jun Pang (*University of Luxembourg*), Yang Zhang (*Saarland University*)
- **Back to the Drawing Board: Revisiting the Design of Optimal Location Privacy-preserving Mechanisms** 1959
Simon Oya (*University of Vigo*), Carmela Troncoso (*IMDEA Software Institute*),
Fernando Pérez-González (*University of Vigo*)

Session I4: Verifying Crypto

- **Certified Verification of Algebraic Properties on Low-Level Mathematical Constructs in Cryptographic Programs** 1973
Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang (*Academia Sinica*)
- **A Fast and Verified Software Stack for Secure Function Evaluation** 1989
José Bacelar Almeida (*INESC TEC & Universidade do Minho*),
Manuel Barbosa (*INESC TEC & FCUP Universidade do Porto*), Gilles Barthe (*IMDEA Software Institute*),
François Dupressoir (*University of Surrey*), Benjamin Grégoire (*Inria Sophia-Antipolis*),
Vincent Laporte (*IMDEA Software Institute*), Vitor Pereira (*INESC TEC & FCUP Universidade do Porto*)
- **Verified Correctness and Security of mbedTLS HMAC-DRBG** 2007
Katherine Q. Ye (*Princeton University & Carnegie Mellon University*),
Matthew Green (*Johns Hopkins University*), Naphat Sanguansin, Lennart Beringer (*Princeton University*),
Adam Petcher (*Oracle*), Andrew W. Appel (*Princeton University*)

Session I5: Communication Privacy

- **How Unique is Your .onion? An Analysis of the Fingerprintability of Tor Onion Services** 2021
Rebekah Overdorf (*Drexel University*), Mark Juarez, Gunes Acar (*imec-COSIC KU Leuven*),
Rachel Greenstadt (*Drexel University*), Claudia Diaz (*imec-COSIC KU Leuven*)
- **The Waterfall of Liberty: Decoy Routing Circumvention that Resists Routing Attacks** 2037
Milad Nasr, Hadi Zolfaghari, Amir Houmansadr (*University of Massachusetts, Amherst*)
- **Compressive Traffic Analysis: A New Paradigm for Scalable Traffic Analysis** 2053
Milad Nasr, Amir Houmansadr, Arya Mazumdar (*University of Massachusetts, Amherst*)

Session J1: Outsourcing

- **Full Accounting for Verifiable Outsourcing** 2071
Riad S. Wahby (*Stanford University*), Ye Ji (*New York University*),
Andrew J. Blumberg (*University of Texas at Austin*), Abhi Shelat (*Northeastern University*),
Justin Thaler (*Georgetown University*), Michael Walfish, Thomas Wies (*New York University*)

- **Ligero: Lightweight Sublinear Arguments Without a Trusted Setup**..... 2087
Scott Ames (*University of Rochester*), Carmit Hazay (*Bar-Ilan University*),
Yuval Ishai (*Technion and University of California, Los Angeles*),
Muthuramakrishnan Venkitasubramaniam (*University of Rochester*)
- **Homomorphic Secret Sharing: Optimizations and Applications** 2105
Elette Boyle (*IDC*), Geoffroy Couteau (*École Normale Supérieure, CNRS, PSL Research University, INRIA*),
Niv Gilboa (*Ben Gurion University*), Yuval Ishai (*Technion and University of California, Los Angeles*),
Michele Orrù (*École Normale Supérieure, CNRS, PSL Research University, INRIA*)

Session J2: Fun with Fuzzing

- **DIFUZE: Interface Aware Fuzzing for Kernel Drivers** 2123
Jake Corina, Aravind Machiry, Christopher Salls (*University of California, Santa Barbara*),
Yan Shoshitaishvili (*Arizona State University*), Shuang Hao (*University of Texas at Dallas*),
Christopher Kruegel, Giovanni Vigna (*University of California, Santa Barbara*)
- **SemFuzz: Semantics-based Automatic Generation of Proof-of-Concept Exploits** 2139
Wei You (*Indiana University, Bloomington*),
Peiyuan Zong, Kai Chen (*Institute of Information Engineering, Chinese Academy of Sciences
& University of Chinese Academy of Sciences*), XiaoFeng Wang (*Indiana University, Bloomington*),
Xiaojing Liao (*William and Mary*), Pan Bian, Bin Liang (*Renmin University of China*)
- **SlowFuzz: Automated Domain-Independent Detection of Algorithmic Complexity Vulnerabilities** 2155
Theofilos Petsios, Jason Zhao, Angelos D. Keromytis, Suman Jana (*Columbia University*)

Session J3: Problematic Patches

- **Identifying Open-Source License Violation and 1-day Security Risk at Large Scale** 2169
Ruian Duan, Ashish Bijlani, Meng Xu, Taesoo Kim, Wenke Lee (*Georgia Institute of Technology*)
- **Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android** 2187
Erik Derr, Sven Bugiel (*Saarland University*), Sascha Fahl, Yasemin Acar (*Leibniz University, Hannover*),
Michael Backes (*Saarland University*)
- **A Large-Scale Empirical Study of Security Patches** 2201
Frank Li, Vern Paxson (*University of California, Berkeley*)

Session J4: Flash Security

- **DEFTL: Implementing Plausibly Deniable Encryption in Flash Translation Layer** 2217
Shijie Jia, Luning Xia (*Chinese Academy of Sciences*), Bo Chen (*Michigan Technological University*),
Peng Liu (*Pennsylvania State University*)
- **FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware** 2231
Jian Huang (*Georgia Institute of Technology*), Jun Xu, Xinyu Xing, Peng Liu (*Pennsylvania State University*),
Moinuddin K. Qureshi (*Georgia Institute of Technology*)
- **FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution** 2245
Grant Hernandez, Farhaan Fowze, Dave (Jing) Tian, Tuba Yavuz, Kevin R. B. Butler (*University of Florida*)

Session K1: Secure Computation

- **TinyOLE: Efficient Actively Secure Two-Party Computation from Oblivious Linear Function Evaluation** 2263
Nico Döttling (*Friedrich-Alexander-University Erlangen-Nürnberg*),
Satrajit Ghosh, Jesper Buus Nielsen, Tobias Nilges, Roberto Trifiletti (*Aarhus University*)

- **Efficient Public Trace and Revoke from Standard Assumptions: Extended Abstract**..... 2277
Shweta Agrawal (*IIT Madras*), Sanjay Bhattacharjee (*Indian Statistical Institute*),
Duong Hieu Phan (*XLIM (U. Limoges, CNRS)*),
Damien Stehlé (*ENS de Lyon, LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL)*),
Shota Yamada (*National Institute of Advanced Industrial Science and Technology (AIST)*)
- **Distributed Measurement with Private Set-Union Cardinality** 2295
Ellis Fenske (*Tulane University*), Akshaya Mani (*Georgetown University*),
Aaron Johnson (*U.S. Naval Research Laboratory*), Micah Sherr (*Georgetown University*)

Session K2: Fuzzing Finer and Faster

- **Designing New Operating Primitives to Improve Fuzzing Performance**..... 2313
Wen Xu, Sanidhya Kashyap (*Georgia Institute of Technology*), Changwoo Min (*Virginia Tech*),
Taesoo Kim (*Georgia Institute of Technology*)
- **Directed Greybox Fuzzing** 2329
Marcel Böhme, Van-Thuan Pham, Manh-Dung Nguyen, Abhik Roychoudhury (*National University of Singapore*)
- **IMF: Inferred Model-based Fuzzer** 2345
HyungSeok Han, Sang Kil Cha (*Korea Advanced Institute of Science and Technology*)

Session K3: Program Analysis

- **PtrSplit: Supporting General Pointers in Automatic Program Partitioning** 2359
Shen Liu, Gang Tan, Trent Jaeger (*Pennsylvania State University*)
- **HexType: Efficient Detection of Type Confusion Errors for C++** 2373
Yuseok Jeon, Priyam Biswas, Scott Carr, Byoungyoung Lee, Mathias Payer (*Purdue University*)
- **FreeGuard: A Faster Secure Heap Allocator** 2389
Sam Silvestro, Hongyu Liu (*University of Texas at San Antonio*), Corey Crosser (*US Military Academy*),
Zhiqiang Lin (*University of Texas at Dallas*), Tongping Liu (*University of Texas at San Antonio*)

Session K4: Secure Enclaves

- **JITGuard: Hardening Just-in-time Compilers with SGX**..... 2405
Tommaso Frassetto, David Gens, Christopher Liebchen, Ahmad-Reza Sadeghi
(*Technische Universität Darmstadt*)
- **Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX** 2421
Wenhao Wang (*Institute of Information Engineering, Chinese Academy of Sciences & Indiana University, Bloomington*), Guoxing Chen (*Ohio State University*),
Xiaorui Pan (*Indiana University, Bloomington*),
Yinqian Zhang (*Ohio State University*), Xiaofeng Wang (*Indiana University, Bloomington*),
Vincent Bindschaedler (*University of Illinois at Urbana-Champaign*),
Haixu Tang (*Indiana University, Bloomington*), Carl A. Gunter (*University of Illinois at Urbana-Champaign*)
- **A Formal Foundation for Secure Remote Execution of Enclaves** 2435
Pramod Subramanyan, Rohit Sinha (*University of California, Berkeley*),
Ilia Lebedev, Srinivas Devadas (*Massachusetts Institute of Technology*),
Sanjit A. Seshia (*University of California, Berkeley*)

Demonstration

- **DEMO: Akatosh: Automated Cyber Incident Verification and Impact Analysis** 2463
Jared M. Smith, Elliot Greenlee (*Oak Ridge National Laboratory & University of Tennessee*),
Aaron Ferber (*Oak Ridge National Laboratory*)

Posters

- **Poster: Adversarial Examples for Classifiers in High-Dimensional Network Data** 2467
Muhammad Ejaz Ahmed, Hyoungshick Kim (*Sungkyunkwan University*)
- **POSTER: An Empirical Measurement Study on Multi-tenant Deployment Issues of CDNs** 2471
Zixi Cai, Zigang Cao, Gang Xiong, Zhen Li, Wei Xia (*Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences*)
- **POSTER: Actively Detecting Implicit Fraudulent Transactions**..... 2475
Shaosheng Cao, XinXing Yang, Jun Zhou, Xiaolong Li, Yuan (Alan) Qi, Kai Xiao (*Ant Financial Services Group*)
- **POSTER: Semi-supervised Classification for Dynamic Android Malware Detection** 2479
Li Chen, Mingwei Zhang, Chih-yuan Yang, Ravi Sahita (*Intel Labs*)
- **POSTER: Detection of CPS Program Anomalies by Enforcing Cyber-Physical Execution Semantics**..... 2483
Long Cheng, Ke Tian, Danfeng (Daphne) Yao (*Virginia Tech*)
- **POSTER: A Comprehensive Study of Forged Certificates in the Wild**..... 2487
Mingxin Cui, Zigang Cao, Gang Xiong, Junzheng Shi (*Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences*)
- **POSTER: Rust SGX SDK: Towards Memory Safety in Intel SGX Enclave**..... 2491
Yu Ding, Ran Duan, Long Li, Yueqiang Cheng, Yulong Zhang, Tanghui Chen (*Baidu X-Lab*), Tao Wei (*Baidu X-Lab*), Huibo Wang (*University of Texas -- Dallas*)
- **POSTER: Finding Vulnerabilities in P4 Programs with Assertion-based Verification**..... 2495
Lucas Freire, Miguel Neves, Alberto Schaeffer-Filho, Marinho Barcellos (*UFRGS*)
- **POSTER: Covert Channel Based on the Sequential Analysis in Android Systems** 2499
Jun-Won Ho, KyungRok Won, Jee Sun Kim (*Seoul Women's University*)
- **POSTER: Why Are You Going That Way? Measuring Unnecessary Exposure of Network Traffic to Nation States**..... 2503
Jordan Holland, Max Schuchard (*University of Tennessee*)
- **POSTER: PriReMat: A Distributed Tool for Privacy Preserving Record Linking in Healthcare** 2507
Diptendu Mohan Kar, Ibrahim Lazrig, Indrajit Ray, Indrakshi Ray (*Colorado State University*)
- **POSTER: AFL-based Fuzzing for Java with Kelinci** 2511
Rody Kersten, Kasper Luckow (*Carnegie Mellon University Silicon Valley*), Corina S. Păsăreanu (*Carnegie Mellon University Silicon Valley & NASA Ames Research Center*)
- **POSTER: Rethinking Fingerprint Identification on Smartphones**..... 2515
Seungyeon Kim, Hoyeon Lee, Taekyoung Kwon (*Yonsei University*)
- **POSTER: X-Ray Your DNS** 2519
Amit Klein (*Fraunhofer Institute for Secure Information Technology*), Vladimir Kravtsov, Alon Perlmuter, Haya Shulman, Michael Waidner (*Fraunhofer Institute for Secure Information Technology & Hebrew University of Jerusalem*)
- **POSTER: Hidden in Plain Sight: A Filesystem for Data Integrity and Confidentiality**..... 2523
Anne Kohlbrenner (*Carnegie Mellon University*), Frederico Araujo, Teryl Taylor, Marc Ph. Stoecklin (*IBM T.J. Watson Research Center*)
- **POSTER: Watch Out Your Smart Watch When Paired** 2527
Youngjoo Lee, WonSeok Yang, Taekyoung Kwon (*Yonsei University*)
- **POSTER: Intrusion Detection System for In-vehicle Networks using Sensor Correlation and Integration**..... 2531
Huaxin Li, Li Zhao, Marcio Juliato, Shabbir Ahmed, Manoj R. Sastry, Lily L. Yang (*Intel Labs*)
- **POSTER: Practical Fraud Transaction Prediction** 2535
Longfei Li, Jun Zhou, Xiaolong Li, Tao Chen (*Ant Financial Services Group*)

- **POSTER: Vulnerability Discovery with Function Representation Learning from Unlabeled Projects** 2539
Guanjun Lin, Jun Zhang, Wei Luo, Lei Pan (*Deakin University*),
Yang Xiang (*Swinburne University of Technology*)
- **POSTER: Neural Network-based Graph Embedding for Malicious Accounts Detection**..... 2543
Ziqi Liu, Chaochao Chen, Jun Zhou, Xiaolong Li, Feng Xu, Tao Chen (*Ant Financial Services Group*),
Le Song (*Ant Financial Services Group & Georgia Institute of Technology*)
- **POSTER: A Unified Framework of Differentially Private Synthetic Data Release with Generative Adversarial Network**..... 2547
Pei-Hsuan Lu, Chia-Mu Yu (*National Chung Hsing University*)
- **POSTER: TOUCHFLOOD: A Novel Class of Attacks against Capacitive Touchscreens** 2551
Seita Maruyama, Satoshiro Wakabayashi, Tatsuya Mori (*Waseda University*)
- **POSTER: TouchTrack: How Unique are your Touch Gestures?**..... 2555
Rahat Masood (*University of New South Wales (UNSW) & CSIRO Data61*),
Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Moahmed Ali Kaafar (*CSIRO Data61*)
- **POSTER: PenJ1939: An Interactive Framework for Design and Dissemination of Exploits for Commercial Vehicles**..... 2559
Subhojeet Mukherjee, Noah Cain, Jacob Walker, David White, Indrajit Ray,
Indrakshi Ray (*Colorado State University*)
- **POSTER: Cyber Attack Prediction of Threats from Unconventional Resources (CAPTURE)**..... 2563
Ahmet Okutan, Gordon Werner, Katie McConky, Shanchieh Jay Yang (*Rochester Institute of Technology*)
- **POSTER: Towards Precise and Automated Verification of Security Protocols in Coq** 2567
Hernan M. Palombo, Hao Zheng, Jay Ligatti (*University of South Florida*)
- **POSTER: Probing Tor Hidden Service with Dockers** 2571
Jonghyeon Park, Youngseok Lee (*Chungnam National University*)
- **POSTER: Evaluating Reflective Deception as a Malware Mitigation Strategy** 2575
Thomas Shaw (*University of Tulsa*), James Arrowood (*Haystack Security LLC*),
Michael Kvasnicka, Shay Taylor, Kyle Cook, John Hale (*University of Tulsa*)
- **POSTER: Improving Anonymity of Services Deployed Over Tor by Changing Guard Selection** 2579
Abhishek Singh (*University of Oslo*)
- **POSTER: Inaudible Voice Commands** 2583
Liwei Song, Prateek Mittal (*Princeton University*)
- **POSTER: Is Active Electromagnetic Side-channel Attack Practical?** 2587
Satoshiro Wakabayashi, Seita Maruyama, Tatsuya Mori, Shigeki Goto (*Waseda University*),
Masahiro Kinugawa (*National Institute of Technology, Sendai College*),
Yu-ichi Hayashi (*Nara Institute of Science and Technology*)
- **POSTER: BGPCoin: A Trustworthy Blockchain-based Resource Management Solution for BGP Security** 2591
Qianqian Xing, Baosheng Wang, Xiaofeng Wang (*National University of Defense Technology*)
- **POSTER: Who was Behind the Camera? — Towards Some New Forensics** 2595
Jeff Yan (*Linköping University*), Aurélien Bourquard (*Massachusetts Institute of Technology*)
- **POSTER: A PU Learning based System for Potential Malicious URL Detection** 2599
Ya-Lin Zhang (*Nanjing University & Ant Financial Services Group*),
Longfei Li, Jun Zhou, Xiaolong Li, Yujiang Liu, Yuanchao Zhang (*Ant Financial Services Group*),
Zhi-Hua Zhou (*Nanjing University*)

Tutorials

- **Identity Related Threats, Vulnerabilities and Risk Mitigation in Online Social Networks** 2603
Leila Bahri (*Royal Institute of Technology - KTH*)
- **Web Tracking Technologies and Protection Mechanisms**..... 2607
Nataliia Bielova (*Université Côte d’Azur, Inria*)
- **Tutorial: Private Information Retrieval** 2611
Ryan Henry (*Indiana University*)
- **CCS’17 Tutorial Abstract / SGX Security and Privacy** 2613
Taesoo Kim (*Georgia Institute of Technology*), Zhiqiang Lin (*University of Texas at Dallas*),
Chia-che Tsai (*Stony Brook University & University of California, Berkeley*)
- **Cliptography: Post-Snowden Cryptography**..... 2615
Qiang Tang (*New Jersey Institute of Technology*), Moti Yung (*Snap Inc. & Columbia University*)
- **Cache Side Channels: State of the Art and Research Opportunities**..... 2617
Yinqian Zhang (*Ohio State University*)

Workshop Summaries

- **10th International Workshop on Artificial Intelligence and Security (AISec 2017)**..... 2621
Battista Biggio (*University of Cagliari*), David Freeman (*Facebook, Inc.*), Brad Miller (*Google Inc.*),
Arunesh Sinha (*University of Michigan*)
- **ASHES 2017— Workshop on Attacks and Solutions in Hardware Security**..... 2623
Chip Hong Chang (*Nanyang Technological University*), Marten van Dijk (*University of Connecticut*),
Farinaz Koushanfar (*University of California, San Diego*), Ulrich Rührmair (*Ruhr-University Bochum*),
Mark Tehranipoor (*University of Florida*)
- **CCSW’17 — 2017 ACM Cloud Computing Security** 2627
Ghassan O. Karame (*NEC Laboratories Europe*), Angelos Stavrou (*George Mason University*)
- **CPS-SPC 2017: Third Workshop on Cyber-Physical Systems Security and PrivaCy** 2629
Rakesh B. Bobba (*Oregon State University*), Awais Rashid (*Lancaster University*)
- **CCS’17 — Women in Cyber Security (CyberW) Workshop**..... 2631
Danfeng (Daphne) Yao (*Virginia Tech*), Elisa Bertino (*Purdue University*)
- **FEAST’17: The 2nd Workshop on Forming an Ecosystem Around Software Transformation..** 2633
Taesoo Kim (*Georgia Institute of Technology*), Dinghao Wu (*Pennsylvania State University*)
- **MIST 2017: 9th International Workshop on Managing Insider Security Threats**..... 2635
Ilsun You (*Soonchunhyang University*), Elisa Bertino (*Purdue University*)
- **MTD 2017: Fourth ACM Workshop on Moving Target Defense (MTD)**..... 2637
Hamed Okhravi (*MIT Lincoln Laboratory*), Xinming Ou (*University of South Florida*)
- **PLAS 2017 – ACM SIGSAC Workshop on Programming Languages and Analysis
for Security** 2639
Nataliia Bielova (*INRIA*), Marco Gaboardi (*University at Buffalo*)
- **SafeConfig’17: Applying the Scientific Method to Active Cyber Defense Research**..... 2641
Nicholas J. Multari (*Pacific Northwest National Lab*),
Anoop Singhal (*National Institute of Standards and Technology*), Erin Miller (*Pacific Northwest National Lab*)
- **16th Workshop on Privacy in the Electronic Society (WPES 2017)** 2643
Adam J. Lee (*University of Pittsburgh*)
- **Workshop on Multimedia Privacy and Security** 2645
Roger Hallman (*US Navy SPAWAR Systems Center Pacific*), Kurt Rohloff (*New Jersey Institute of Technology*),
Victor Chang (*Xian Jiaotong Liverpool University*)
- **IoT S&P 2017: First Workshop on Internet of Things Security and Privacy** 2647
Theophilus Benson (*Brown University*), Peng Liu (*Penn State University*),
Srikanth Sundaresan (*Princeton University*), Yuqing Zhang (*University of Chinese Academy of Sciences*)

- **Author Index** 2649

CCS 2017 Conference Organization

General Chair: Bhavani Thuraisingham (*The University of Texas at Dallas*)

Program Chairs: David Evans (*University of Virginia*)
Tal Malkin (*Columbia University*)
Dongyan Xu (*Purdue University*)

Workshops Chairs: Taesoo Kim (*Georgia Tech*)
Cliff Wang (*Army Research Office*)

Tutorial Chairs: Guofei Gu (*Texas A&M*)
Maribel Fernandez (*Kings College, University of London*)

Poster/Demo Chairs: Kevin Hamlen (*The University of Texas at Dallas*)
Heng Yin (*University of California, Riverside*)

Treasurer: Alvaro Cardenas (*The University of Texas at Dallas*)

Web Chairs: JV Rajendran (*The University of Texas at Dallas*)
Gail-Joon Ahn (*Arizona State University*)

Panel Chairs: Ahmad-Reza Sadeghi (*TU Darmstadt, CYSEC*)
Yiorgos Makris (*The University of Texas at Dallas*)

Registration Chair: Murat Kantarcioglu (*The University of Texas at Dallas*)

Student Travel Grant Chairs: Hassan Takabi (*University of North Texas*)
Brent Kang (*KAIST*)
Zhi Wang (*Florida State University*)

Publicity Chair: Yvo Desmedt (*The University of Texas at Dallas*)
Giancarlo Pellegrino (*Saarland University*)
Daniel Xiapu Luo (*The Hong Kong Polytechnic University*)
Barbara Carminati (*University of Insubria*)

Social Media Chair: Siddharth Garg (*New York University*)

Proceedings Chairs: Matthew Wright (*Rochester Institute of Technology*)
Apu Kapadia (*Indiana University Bloomington*)

Sponsor/Industry Outreach Chairs: Janell Straach (*The University of Texas at Dallas*)
Peng Liu (*Penn State University*)
Gail-Joon Ahn (*Arizona State University*)

Local Arrangement Chairs: Zhiqiang Lin (*The University of Texas at Dallas*)
Rhonda Walls (*The University of Texas at Dallas*)

Volunteer Coordinator/Chairs: Latifur Khan (*The University of Texas at Dallas*)
Meera Sridhar (*University of North Carolina at Charlotte*)

Program Committee: Sadia Afroz, (*UC Berkeley / ICSI*)
Gail-Joon Ahn (*Arizona State University*)
Ehab Al-Shaer (*University of North Carolina Charlotte*)
Elias Athanasopoulos (*University of Cyprus*)
Foteini Baldimtsi (*George Mason University*)
David Basin (*ETH Zurich*)
Adam Bates (*University of Illinois at Urbana-Champaign*)
Lujó Bauer (*Carnegie Mellon University*)
Konstantin Beznosov (*University of British Columbia*)
Karthikeyan Bhargavan (*INRIA*)
Alex Biryukov (*University of Luxembourg*)
Jeremiah Blocki (*Purdue University*)
Elette Boyle (*IDC Herzliya*)
Levente Buttyán (*CrySyS Lab (BME)*)
Juan Caballero (*IMDEA Software Institute*)
Joseph Calandrino (*Federal Trade Commission*)
Aylin Caliskan (*Princeton University*)
Yinzhi Cao (*Lehigh University*)
Alvaro A. Cardenas (*University of Texas at Dallas*)
Lorenzo Cavallaro (*Royal Holloway, University of London*)
Neha Chachra (*Facebook*)
Melissa Chase (*Microsoft Research*)
Haibo Chen (*Shanghai Jiao Tong University*)
Hao Chen (*University of California, Davis*)
Omar Chowdhury (*University of Iowa*)
Nicolas Christin (*Carnegie Mellon University*)
Véronique Cortier (*Loria (CNRS (France))*)
Manuel Costa (*Microsoft Research*)
Scott Coull (*FireEye*)
Weidong Cui (*Microsoft Research*) Anupam
Das (*Carnegie Mellon University*) Anupam
Datta (*Carnegie Mellon University*) Lucas
Davi (*University of Duisburg-Essen*)
Emiliano De Cristofaro (*University College London*)
Tamara Denning (*University of Utah*)
Xuhua Ding (*Singapore Management University*)
Brendan Dolan-Gavitt (*New York University*)
Adam Doupe (*Arizona State University*)

Program Committee (continued): Tudor Dumitraş (*University of Maryland*)
Serge Egelman (*UC Berkeley / ICSI*)
Ittay Eyal (*Cornell University*)
Sascha Fahl (*Saarland University*)
Christopher Fletcher (*NVIDIA/UIUC*)
Aurélien Francillon (*EURECOM*)
Matt Fredrikson (*Carnegie Mellon University*)
Xinyang Ge (*Microsoft Research*)
Daniel Genkin (*University of Pennsylvania / University of Maryland*)
Rosario Gennaro (*City College of New York*)
Phillipa Gill (*University of Massachusetts Amherst*)
Dov Gordon (*George Mason University*)
Andreas Haeberlen (*University of Pennsylvania*)
J. Alex Halderman (*University of Michigan*)
Shai Halevi (*IBM Research*)
Matthew Hicks (*MIT Lincoln Laboratory*)
Michael Hicks (*University of Maryland*)
Thorsten Holz (*Ruhr-Universität Bochum*)
Amir Houmansadr (*University of Massachusetts Amherst*)
Yan Huang (*Indiana University*)
Kyu Hyung Lee (*University of Georgia*)
Trent Jaeger (*Penn State University*)
Suman Jana (*Columbia University*)
Limin Jia (*Carnegie Mellon University*)
Yier Jin (*University of Central Florida*)
Aaron Johnson (*U.S. Naval Research Laboratory*)
Philipp Jovanovic (*École Polytechnique Fédérale de Lausanne*)
Brent ByungHoon Kang (*KAIST*)
Aniket Kate (*Purdue University*)
Jonathan Katz (*University of Maryland*)
Stefan Katzenbeisser (*TU Darmstadt*)
Marcel Keller (*University of Bristol*)
Aggelos Kiayias (*University of Edinburgh*)
Taesoo Kim (*Georgia Tech*)
Yongdae Kim (*KAIST*)
Engin Kirda (*Northeastern University*)
David Kotz (*Dartmouth*)
Farinaz Koushanfar (*UC San Diego*)
Ralf Küsters (*University of Stuttgart*)
Andrea Lanzi (*University of Milan*)
Byoungyoung Lee (*Purdue University*)
Wenke Lee (*Georgia Tech*)
Brian N. Levine (*University of Massachusetts Amherst*)
Zhichun Li (*NEC Labs*)

Program Committee (continued): Zhou Li (*RSA*)
David Lie (*University of Toronto*)
Yao Liu (*University of South Florida*)
Matteo Maffei (*TU Vienna*)
Mohammad Mahmody (*University of Virginia*)
Z. Morley Mao (*University of Michigan*)
Ivan Martinovic (*University of Oxford*)
Michelle L. Mazurek (*University of Maryland*)
Jonathan McCune (*Google*)
Andrew Miller (*University of Illinois at Urbana-Champaign*)
Tal Moran (*IDC Herzliya*)
Muhammad Naveed (*University of Southern California*)
Nick Nikiforakis (*Stony Brook University*)
Hamed Okhravi (*MIT Lincoln Laboratory*)
Alina Oprea (*Northeastern University*)
Mathias Payer (*Purdue University*)
Adrian Perrig (*ETH Zurich*)
Michalis Polychronakis (*Stony Brook University*)
Georgios Portokalidis (*Stevens Institute of Technology*)
Bart Preneel (*KU Leuven*)
Zhiyun Qian (*University of California, Riverside*)
Kasper Rasmussen (*University of Oxford*)
Aseem Rastogi (*Microsoft Research India*)
Mariana Raykova (*Yale University*)
Kaveh Razavi (*Vrije Universiteit*)
William Robertson (*Northeastern University*)
Christian Rossow (*Saarland University*)
Mike Rosulek (*Oregon State University*)
Patrick Schaumont (*Virginia Tech*)
abhi shelat (*Northeastern*)
Micah Sherr (*Georgetown University*)
Timothy Sherwood (*UC Santa Barbara*)
Reza Shokri (*Cornell Tech*)
Stelios Sidiroglou-Douskos (*MIT*)
Chengyu Song (*UC Riverside*)
Douglas Stebila (*McMaster University*)
Deian Stefan (*UC San Diego*)
Gianluca Stringhini (*University College London*)
Kun Sun (*George Mason University*)
Ewa Syta (*Trinity College*)
Mohit Tiwari (*UT Austin*)
Patrick Traynor (*University of Florida*)
Carmela Troncoso (*IMDEA Software Institute*)
Blase Ur (*University of Chicago*)

Program Committee (continued): Marten van Dijk (*University of Connecticut*)
Haining Wang (*University of Delaware*)
XiaoFeng Wang (*Indiana University*)
Zhi Wang (*Florida State University*)
Matthew Wright (*Rochester Institute of Technology*)
Dinghao Wu (*Pennsylvania State University*)
Zhenyu Wu (*NEC Laboratories America*)
Luyi Xing (*Indiana University*)
Xinyu Xing (*Pennsylvania State University*)
Guanhua Yan (*Binghamton University*)
Lok Yan (*Air Force Research Laboratory*)
Heng Yin (*University of California, Riverside*)
Samee Zahur (*Google*)
Fengwei Zhang (*Wayne State University*)
Kehuan Zhang (*Chinese University of Hong Kong*)
Yanchao Zhang (*Arizona State University*)
Yinqian Zhang (*The Ohio State University*)
Sencun Zhu (*Pennsylvania State University*)
Saman Zonouz (*Rutgers University*)

Additional reviewers: Hadi Abdullah	Pyrros Chaidos
Gergely Ács	Konstantinos Chatzikokolakis
David Adrian	Sze Yiu Chau
Eman Alashwali	Ying Chen
Joey Allen	Shang-Tse Chen
Myrto Arapinis	Haehyun Cho
Jean-Philippe Aumasson	Pak Ho Chung
Christian Badertscher	Katriel Cohn Gordon
Xiaolong Bai	Christian Decker
Qinkun Bao	Zakir Durumeric
Cristina Basescu	Mohammad Etemad
Aditya Basu	Daniel Feher
Carsten Baum	Daniel Fett
Ingolf Becker	Hao Fu
Matt Bernhard	Yu Fu
Shengjie Bi	Joshua Gancher
Gergely Biczók	linus gasser
Jorje Blasco Alis	Linus Gasser
Logan Blue	András Gazdag
Jasmin Bowers	David Gens
Ferdinand Brasser	Ilias Giechaskiel
Ahmet S. Buyukkayhan	Thomas Gilray
Frank Capoblanco	Liang Gong
Sunjay Cauligi	Sergey Gorbunov

Additional reviewers (*continued*): Wenbo Guo
Johann Großschädl
Trinabh Gupta
Syed Kamran Haider
Ariel Hamlin
Wajih Ul Hassan
Ben Heidorn
Ethan Heilman
Nadia Heninger
Tamás Holczer
Hongxin Hu
Hong Hu
Heqing Huang
Zhen Huang
Jun Ho Huh
Siam Hussain
Yong Ho Hwang
Ahmad Ibrahim
Moshen Imani
Yuval Ishai
Saman Jafari
Stanislaw Jarecki
Roberto Jordaney
Ryo Kikuchi
Donguk Kim Beom
Heyn Kim
Markulf Kohlweiss
Eleftherios Kokoris Kogias
Maria Konte
Lucas Kowalczyk
Steve Kremer
Bogdan Kulynych
Yu-Tsung (Eddy) Lee
Yue Li
Tongxin Li
Xiaojing Liao
Christopher Liechen
Yehuda Lindell
Xiao Liu
Andreas Lochbihler
Wouter Lueks
Andrea Mambretti
Piotr Mardziel
Christian Matt
Xianghang Mi
Reza Mirzazade
Varun Mishra
Esfandiar Mohammadi
Pedro Moreno Sanchez
Johannes Müller
Kartik Nayak
Kirill Nikitin
Ben Niu
Rebekah Overdorf
Simón Oya
Jun Pang
Dimitrios Papadopoulos
Charalampos Papamanthou
Bryan Parno
Marcus Peinado
Travis Peters
Giuseppe Petracca
Tim Pierson
Benny Pinkas
Yu Pu
Apostolos Pyrgelis
Rui Qiao
Samuel Ranellucci
Daniel Rausch
Bradley Reaves
M. Sadegh Riazi
Silas Richelson
Marc Roeschlin
Kurt Rohloff
Carlos Rubio Medrano
Ralf Sasse
Nolen Scaife
Guillaume Scerri
Guido Schmitz
Peter Scholl
Will Scott
Sovantharith Seng
Daniele Sgandurra

Additional reviewers (<i>continued</i>):	Junbum Shin	Li Wang
	Victor Shoup	Xueqiang Wang
	Payap Sirinam	Wenhao Wang
	Gary Soeller	Bogdan Warinschi
	Linhai Song	Daniel Wicks
	Ebrahim Songhori	Michelle Wong
	Christoph Sprenger	David Wu
	Drew Springall	Xiaodi Wu
	Rock Stevens	Eric Wustrow
	Yuqiong Sun	Willem Wyndham
	Jianhua Sun	Weilin Xu
	Pengfei Sun	Zhang Xu
	Peter Yi Ping Sun	Dongpeng Xu
	Zhibo Sun	Carter Yagemann
	Stefano Tessaro	Moosa Yahyazadeh
	Jonathan Ullman	Yang Yang
	Diego Valasquez	Insu Yun
	Ben VanderSloot	Santiago Zanella
	Luis Vargas	Béguelin
	Daniel Votipka	Danfeng Zhang
	Kyle Wallace	Ning Zhang
	Shengye Wan	Tianwei Zhang
	Boyang Wang	Xiaokuan Zhang
	Pei Wang	Kaixuan Zhang
	Shuai Wang	Ziming Zhao
	Xiao Wang	Yajin Zhou
	Qinglong Wang	Ruiyu Zhu
	Weiren Wang	