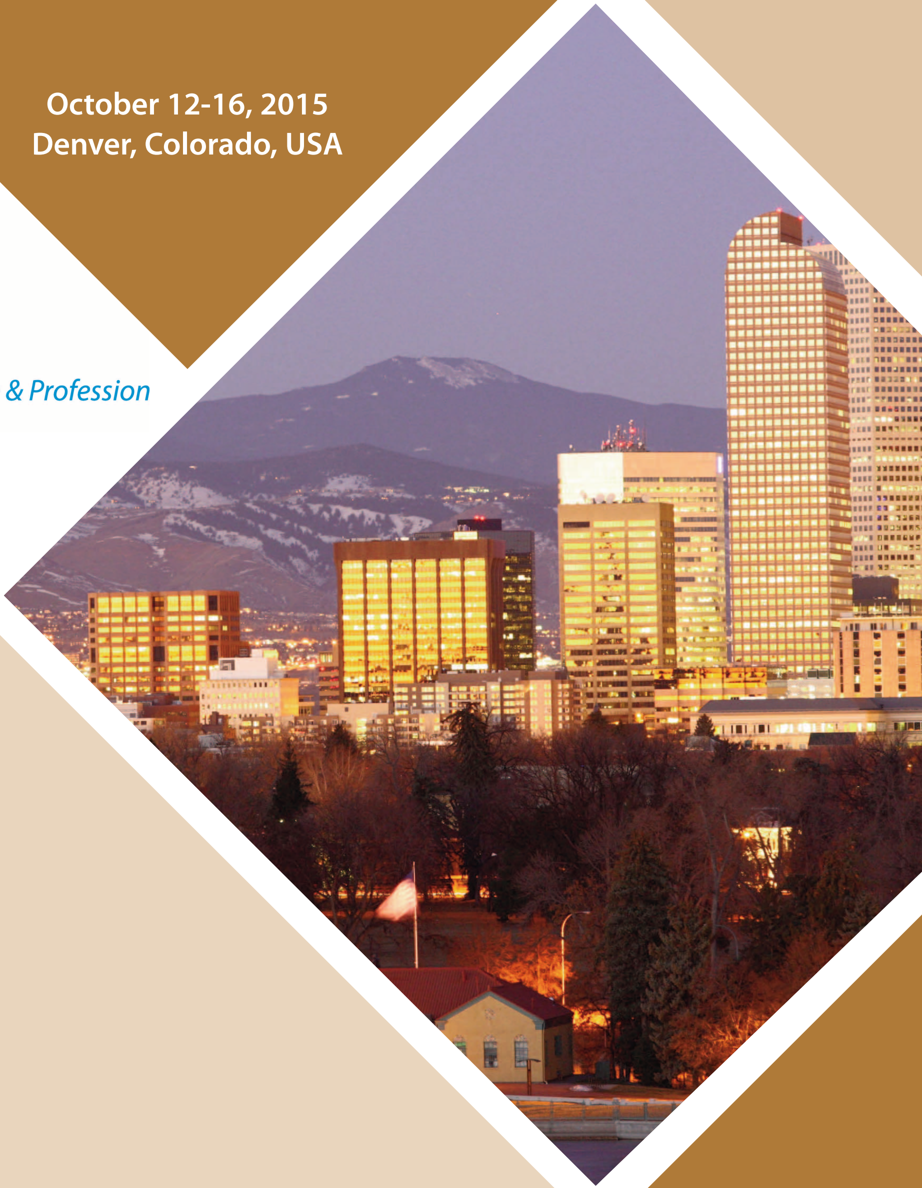
October 12-16, 2015
Denver, Colorado, USA

Association for
Computing Machinery

Advancing Computing as a Science & Profession



CCS'15

Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security

Sponsored by:

ACM SIGSAC

Supported by:

National Science Foundation, US Army Research Office, CISCO, SAP, Microsoft Research, Google, Hewlett-Packard, IBM Research, Colorado State University, & Arizona State University

Association for
Computing Machinery

Advancing Computing as a Science & Profession

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

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: 978-1-4503-3832-5

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 2015 General Chair’s Welcome

I take this opportunity to welcome you to the 22nd Annual ACM Conference on Computer and Communications Security (CCS 2015). It has been an honor for me to provide leadership to this conference. The mission of CCS is to bring together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. From its inception, CCS has established itself as a high standard research conference in its area. This year’s CCS event continues this long tradition with a very strong technical program comprising 12 technical sessions, 3 tutorials, 28 posters/demos, 10 specialized pre- and post-conference workshops and talks by distinguished invited speakers.

Organizing such a prestigious conference is never a solo effort and I have been very fortunate to receive incredible help and support from many colleagues. I would first like to thank all the authors without whose dedication and commitment to security research this conference would never have been possible. At the same time, I would like to thank Christopher Kruegel and Ninghui Li, the Program Chairs, and members of the Program Committee for their hard work in peer-reviewing and critiquing the papers for the research track and putting together a strong program.

I would like to extend this appreciation to the Workshop Chairs, Xiaofeng Wang and Kui Ren, for providing leadership to the CCS 2015 workshops, as well as to the respective Workshop Program Chairs and Program Committees – David Lee and Glenn Wurster (SPSM 2015), Nicholas Hopper and Rob Jansen (WPES 2015), Ehab Al-Shaer, Christopher Oehmen and Mohammad Ashiqur Rahman (SafeConfig 2015), Tomas Sander and Moti Yung (WISCS 2015), George Cybenko and Dijiang Huang (MTD 2015), Elisa Bertino and Ilsun You (MIST 2015), Christina Nita-Rotaru and Florian Kerschbaum (CCSW 2015), Christos Dimitrakakis, Katerina Mitrokotsa and Arunesh Sinha (AISec 2015), Rakesh Bobba, Alvaro Cardenas and Roshan Thomas (CPS-SPC 2015) and Jorge Guajardo and Stefan Katzenbeisser (TrustED 2015). Special thanks to Xinming Ou, Sachin Shetty and Anna Squicciarini for their hard work as Poster/Demo Chairs and James Joshi, Rinku Dewri and Patrick Tague for their hard work as Tutorial Chairs. Many thanks to the CCS 2015 Steering Committee chaired by Somesh Jha and ACM SIGSAC chaired by Trent Jaeger.

I am very grateful to members of the Organizing Committee – Yu Chen (Treasurer), Indrakshi Ray and Hasan Takabi (Student Travel Grant Chairs), Feng Li and Tarik Moataz (Publications Chairs), Chuan Yue and Stacy Karas (Web Chairs), Alex Sprintson and Mikhail Strizhov (Registration Chairs), and Dongwan Shin and Dieudonne Mulamba (Publicity Chairs). Thanks to Christos Papadopoulos as Sponsor/Industry Outreach Chair and Ramki Thurimella and Edward Chow for help with local arrangements. I would also like to acknowledge the administrative staff of ACM, ACM SIGSAC, Colorado State University, George Mason University and the Denver Marriott City Center for smooth running of the conference.

Last but not least, I would like to specially thank the following institutions for their generous financial support to 2015 ACM CCS – the U.S. National Science Foundation, the Army Research Office, Cisco, SAP, Microsoft Research, Google, HP Labs, IBM Research, and Arizona State University.

Indrajit Ray
General Chair, CCS 2015
Colorado State University, USA

CCS 2015 Program Chairs’ Welcome

We are pleased to present herein the proceedings of the 2015 ACM Conference on Computer and Communications Security (CCS 2015), held in Denver, Colorado, USA, October 12-16, 2015.

We received 660 submissions (not including some initial withdrawals). This is the largest number of submissions received to date by a computer security conference. A Program Committee comprising 120 experts from 20 countries, helped by 338 external reviewers, evaluated these submissions, employing the customary double-blind review procedure. The review process resulted in 128 papers being accepted to the program (with authors from 19 countries), representing an acceptance rate of about 19.4% and providing a very broad coverage of the entire information security area.

The review process was organized in three phases. After a first review phase, the authors of each paper were sent at least two preliminary reviews (the vast majority of papers, in fact, got three reviews). Authors were given an opportunity to respond to the comments received. During the second phase, reviews were updated as necessary, and, in some cases, additional reviews were solicited. The first and third phases included comprehensive discussions, and after an intensive final debate, the acceptance decisions were made.

This year, we introduced a rebuttal task force, whose 15 members were selected from the Program Committee. The goal of this task force was to go over all the authors’ responses (rebuttals) received in the second phase and to ensure that the reviewers properly addressed all valid concerns that the authors had raised. We hope that most authors benefitted from the feedback received from the CCS reviewers, and that the review process has helped them improve their papers (while we are also aware that due to the short reviewing time, at a conference of CCS scale it is unavoidable that a handful of reviews may be possibly lacking in some respect).

We are very grateful to the members of the Program Committee for their very hard work, professionalism, and responsiveness under very tight deadline requirements. On average, each individual reviewed 18 papers, and nearly a third of the members volunteered to help shepherd accepted papers toward improved presentations. Most members engaged in lively discussions on, both, submissions and author responses, and updated their reviews to reflect valuable insights derived from those discussions. We are also indebted to the external reviewers whose focused expertise added substantial value to the feedback for authors. Moreover, we want to thank the CCS 2015 conference committee: the general chair, workshop/ poster/ tutorial co-chairs, and other chairs and organizers, as well as the steering committee, for numerous discussions on how to produce an exceptional program and for their hard work on the production of these proceedings.

Lastly, we thank the authors of all submitted papers, and all attendees for their participation in the technical discussion during the conference. We hope that you find the program stimulating, enjoyable, and helpful in advancing the exciting area of computer and communication security.

Ninghui Li
ACM CCS’15 Program Co-Chair
Purdue University, USA

Christopher Kruegel
ACM CCS’15 Program Co-Chair
University of California at Santa Barbara, USA

Table of Contents

ACM CCS 2015 Conference Organization xviii

ACM CCS 2015 Sponsor & Supporters xiv

Keynote Talks

- **From Mental Poker to Core Business: Why and How to Deploy Secure Computation Protocols?** 1
  Moti Yung *(Google Inc. & Columbia University)*
- **Keynote Speaker's Bio** 3
  Edward Felten *(Princeton University)*

Session 1A: How Real World Crypto Fails

- **Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice** 5
  David Adrian *(University of Michigan),* Karthikeyan Bhargavan *(INRIA Paris-Rocquencourt),*
  Zakir Durumeric *(University of Michigan),* Pierrick Gaudry *(INRIA Nancy-Grand Est, CNRS &Université de Lorraine),*
  Matthew Green *(Johns Hopkins University),* J. Alex Halderman *(University of Michigan),*
  Nadia Heninger *(University of Pennsylvania),* Drew Springall *(University of Michigan),*
  Emmanuel Thomé *(INRIA Nancy-Grand Est, CNRS and Université de Lorraine),*
  Luke Valenta *(University of Pennsylvania),* Benjamin VanderSloot *(University of Michigan),*
  Eric Wustrow *(University of Michigan),* Santiago Zanella-Béguelin *(Microsoft Research),*
  Paul Zimmermann *(INRIA Nancy-Grand Est, CNRS and Université de Lorraine)*
- **Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards** 18
  Carlo Meijer, Roel Verdult *(Radboud University)*

Session 1B: MAC OS and iOS Security

- **Cracking App Isolation on Apple: Unauthorized Cross-App Resource Access on MAC OS X and iOS** 31
  Luyi Xing *(Indiana University Bloomington),* Xiaolong Bai *(Indiana Univ.Bloomington & Tsinghua University),*
  Tongxin Li *(Peking University),* XiaoFeng Wang *(Indiana University Bloomington),*
  Kai Chen *(Indiana University Bloomington & Chinese Academy of Sciences),*
  Xiaojing Liao *(Georgia Institute of Technology),* Shi-Min Hu *(Tsinghua University),*
  Xinhui Han *(Peking University)*
- **iRiS: Vetting Private API Abuse in iOS Applications** 44
  Zhui Deng, Brendan Saltaformaggio, Xiangyu Zhang, Dongyan Xu *(Purdue University)*

Session 1C: Censorship and Resistance

- **Seeing through Network-Protocol Obfuscation** 57
  Liang Wang *(University of Wisconsin-Madison),* Kevin P. Dyer *(Portland State University),*
  Aditya Akella *(University of Wisconsin-Madison),* Thomas Ristenpart *(Cornell Tech),*
  Thomas Shrimpton *(University of Florida)*
- **CacheBrowser: Bypassing Chinese Censorship without Proxies Using Cached Content** 70
  John Holowczak, Amir Houmansadr *(University of Massachusetts, Amherst)*

Session 2A: Authenticated Encryption

- **Automated Analysis and Synthesis of Authenticated Encryption Schemes** 84
  Viet Tung Hoang *(University of Maryland, Georgetown University),*
  Jonathan Katz, Alex J. Malozemoff *(University of Maryland)*
- **Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives** 96
  Olivier Pereira, François-Xavier Standaert *(Université catholique de Louvain),*
  Srinivas Vivek *(University of Luxembourg & University of Bristol)*
- **GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte** 109
  Shay Gueron *(University of Haifa and Intel Corporation),* Yehuda Lindell *(Bar-Ilan University)*

Session 2B: Android and Web Forensics

- **GUITAR: Piecing Together Android App GUIs from Memory Images** 120
  Brendan Saltaformaggio, Rohit Bhatia, Zhongshu Gu, Xiangyu Zhang, Dongyan Xu *(Purdue University)*
- **WebCapsule: Towards a Lightweight Forensic Engine for Web Browsers** 133
  Christopher Neasbitt, Bo Li *(University of Georgia),*
  Roberto Perdisci *(University of Georgia & Georgia Tech),*
  Long Lu *(Stony Brook University),* Kapil Singh *(IBM Research),* Kang Li *(University of Georgia)*
- **VCR: App-Agnostic Recovery of Photographic Evidence from Android Device Memory Images** 146
  Brendan Saltaformaggio, Rohit Bhatia, Zhongshu Gu, Xiangyu Zhang, Dongyan Xu *(Purdue University)*

Session 2C: Password Security

- **Monte Carlo Strength Evaluation: Fast and Reliable Password Checking** 158
  Matteo Dell'Amico *(Symantec Research Labs)*, Maurizio Filippone *(University of Glasgow)*
- **Surpass: System-initiated User-replaceable Passwords** 170
  Jun Ho Huh *(Honeywell ACS Labs),* Seongyeol Oh, Hyoungshick Kim *(Sungkyunkwan University)*,
  Konstantin Beznosov *(University of British Columbia),*
  Apurva Mohan, S. Raj Rajagopalan *(Honeywell ACS Labs)*
- **Optimal Distributed Password Verification** 182
  Jan Camenisch, Anja Lehmann, Gregory Neven *(IBM Research - Zurich)*

Session 3A: Using CryptoCurrency

- **How to Use Bitcoin to Play Decentralized Poker** 195
  Ranjit Kumaresan *(Massachusetts Institute of Technology),* Tal Moran *(IDC Herzliya),*
  Iddo Bentov *(Technion)*
- **Micropayments for Decentralized Currencies** 207
  Rafael Pass *(Cornell Tech),* abhi shelat *(University of Virginia)*
- **Liar, Liar, Coins on Fire!: Penalizing Equivocation by Loss of Bitcoins** 219
  Tim Ruffing *(Saarland University),* Aniket Kate *(Purdue University),*
  Dominique Schröder *(Saarland University)*
- **Traitor Deterring Schemes: Using Bitcoin as Collateral for Digital Content** 231
  Aggelos Kiayias *(National and Kapodistrian University of Athens),*
  Qiang Tang *(University of Connecticut)*

Session 3B: Memory Randomization

- **It's a TRaP: Table Randomization and Protection against Function-Reuse Attacks** 243
  Stephen Crane *(University of California, Irvine),* Stijn Volckaert *(Universiteit Gent, Belgium),*
  Felix Schuster *(HGI, Ruhr-Universität Bochum),* Christopher Liebchen *(CASED/Technishe Universität Darmstadt),*
  Per Larsen *(University of California, Irvine),*
  Lucas Davi, Ahmad-Reza Sadeghi *(CASED, Technische Universität Darmstadt),*
  Thorsten Holz *(HGI, Ruhr-Universität Bochum),* Bjorn De Sutter *(Universiteit Gent, Belgium),*
  Michael Franz *(University of California, Irvine)*
- **Heisenbyte: Thwarting Memory Disclosure Attacks using Destructive Code Reads** 256
  Adrian Tang, Simha Sethumadhavan, Salvatore Stolfo *(Columbia University)*
- **Timely Rerandomization for Mitigating Memory Disclosures** 268
  David Bigelow, Thomas Hobson, Robert Rudd, William Streilein, Hamed Okhravi *(MIT Lincoln Laboratory)*
- **ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks** 280
  Kangjie Lu, Chengyu Song, Byoungyoung Lee, Simon P. Chung, Taesoo Kim,
  Wenke Lee *(Georgia Institute of Technology)*

Session 3C: Wireless and VoLTE Security

- **Location-restricted Services Access Control Leveraging Pinpoint Waveforming** 292
  Tao Wang, Yao Liu *(University of South Florida),* Qingqi Pei *(Xidian University),*
  Tao Hou *(University of South Florida)*
- **SafeDSA: Safeguard Dynamic Spectrum Access against Fake Secondary Users** 304
  Xiaocong Jin, Jingchao Sun *(Arizona State University),* Rui Zhang *(University of Hawaii),*
  Yanchao Zhang *(Arizona State University)*
- **Insecurity of Voice Solution VoLTE in LTE Mobile Networks** 316
  Chi-Yu Li, Guan-Hua Tu *(University of California, Los Angeles),* Chunyi Peng *(The Ohio State University),*
  Zengwen Yuan, Yuanjie Li, Songwu Lu *(University of California, Los Angeles),*
  Xinbing Wang *(Shanghai Jiao Tong University)*
- **Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations** 328
  Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han *(Korea Advanced Institute of Science & Technology),*
  Yeongjin Jang *(Georgia Institute of Technology),*
  Dongsu Han *(Korea Advanced Institute of Science and Technology),*
  Taesoo Kim *(Georgia Institute of Technology),* Yongdae Kim *(Korea Advanced Institute of Science &Technology)*

Session 4A: Applied Crypto

- **Defeating IMSI Catchers** 340
  Fabian van den Broek, Roel Verdult *(Radboud University),* Joeri de Ruiter *(University of Birmingham)*
- **DEMOS-2: Scalable E2E Verifiable Elections without Random Oracles** 352
  Aggelos Kiayias, Thomas Zacharias *(National and Kapodistrian University of Athens),*
  Bingsheng Zhang *(Lancaster University)*
- **Subversion-Resilient Signature Schemes** 364
  Giuseppe Ateniese, Bernardo Magri, Daniele Venturi *(Sapienza University of Rome)*
- **Walls Have Ears! Opportunistically Communicating Secret Messages Over the Wiretap Channel: from Theory to Practice** 376
  Qian Wang *(Wuhan University),* Kui Ren *(The State University of New York at Buffalo and Jinan University),*
  Guancheng Li, Chenbo Xia, Xiaobing Chen, Zhibo Wang, Qin Zou *(Wuhan University)*

Session 4B: Software Vulnerabilities

- **Static Detection of Packet Injection Vulnerabilities – A Case for Identifying Attacker-controlled Implicit Information Leaks** 388
  Qi Alfred Chen *(University of Michigan),* Zhiyun Qian *(University of California Riverside),*
  Yunhan Jack Jia, Yuru Shao, Z. Morley Mao *(University of Michigan)*
- **Unearthing Stealthy Program Attacks Buried in Extremely Long Execution Paths** 401
  Xiaokui Shu, Danfeng Yao, Naren Ramakrishnan *(Virginia Tech)*
- **From Collision to Exploitation: Unleashing Use-After-Free Vulnerabilities in Linux Kernel** 414
  Wen Xu, Juanru Li, Junliang Shu, Wenbo Yang, Tianyi Xie, Yuanyuan Zhang, Dawu Gu
  (Shanghai Jiao Tong University)
- **VCCFinder: Finding Potential Vulnerabilities in Open-Source Projects to Assist Code Audits** 426
  Henning Perl *(Fraunhofer FKIE),* Sergej Dechand *(University of Bonn),*
  Matthew Smith *(Fraunhofer FKIE and University of Bonn),*
  Daniel Arp, Fabian Yamaguchi, Konrad Rieck *(University of Göttingen),*
  Sascha Fahl, Yasemin Acar *(Saarland University)*

Session 4C: Assessing Current Defences

- **UCognito: Private Browsing without Tears** 438
  Meng Xu, Yeongjin Jang, Xinyu Xing, Taesoo Kim, Wenke Lee *(Georgia Institute of Technology)*
- **Security by Any Other Name: On the Effectiveness of Provider Based Email Security** 450
  Ian Foster, Jon Larson, Max Masich, Alex C. Snoeren, Stefan Savage,
  Kirill Levchenko *(University of California, San Diego)*
- **Certified PUP: Abuse in Authenticode Code Signing** 465
  Platon Kotzias *(IMDEA Software Institute & Universidad Politécnica de Madrid),*
  Srdjan Matic *(Universita degli Studi di Milano),*
  Richard Rivera *(IMDEA Software Institute & Universidad Politécnica de Madrid),*
  Juan Caballero *(IMDEA Software Institute)*
- **A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings** 479
  Ajaya Neupane *(University of Alabama at Birmingham),* Md. Lutfor Rahman *(Aegis Foundry LLC),*
  Nitesh Saxena *(University of Alabama at Birmingham),* Leanne Hirshfield *(Syracuse University)*

Session 5A: Computing on Encrypted Data

- **Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance** 492
  Xiao Shaun Wang *(University of Maryland),*
  Yan Huang, Yongan Zhao, Haixu Tang, XiaoFeng Wang, Diyue Bu *(Indiana University)*
- **GRECS: Graph Encryption for Approximate Shortest Distance Queries** 504
  Xianrui Meng *(Boston University),* Seny Kamara *(Microsoft Research),*
  Kobbi Nissim *(Ben-Gurion University, CRCS Harvard University),* George Kollios *(Boston University)*

Session 5B: Understanding Android Apps

- **Towards Automatic Generation of Security-Centric Descriptions for Android Apps** 518
  Mu Zhang *(NEC Laboratories America, Inc.),* Yue Duan, Qian Feng, Heng Yin *(Syracuse University)*
- **AUTOREB: Automatically Understanding the Review-to-Behavior Fidelity in Android Applications** 530
  Deguang Kong *(Samsung Research America),* Lei Cen *(Purdue University),*
  Hongxia Jin *(Samsung Research America)*

Session 5C: Scanning the Web

- **A Search Engine Backed by Internet-Wide Scanning** 542
  Zakir Durumeric, David Adrian, Ariana Mirian *(University of Michigan),* Michael Bailey *(University of Illinois),*
  J. Alex Halderman *(University of Michigan)*

- **Sunlight: Fine-grained Targeting Detection at Scale with Statistical Confidence** 554
  Mathias Lecuyer, Riley Spahn, Yannis Spiliopolous, Augustin Chaintreau, Roxana Geambasu,
  Daniel Hsu *(Columbia University)*

Session 6A: Garbled Circuits

- **Fast Garbling of Circuits Under Standard Assumptions** 567
  Shay Gueron *(University of Haifa and Intel Corporation),*
  Yehuda Lindell, Ariel Nof, Benny Pinkas *(Bar-Ilan University)*

- **Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries** 579
  Yehuda Lindell, Ben Riva *(Bar-Ilan University)*

- **Fast and Secure Three-party Computation: the Garbled Circuit Approach** 591
  Payman Mohassel *(Yahoo Labs),* Mike Rosulek *(Oregon State University),* Ye Zhang *(Google Inc.)*

Session 6B: Web Application Security

- **FlowWatcher: Defending against Data Disclosure Vulnerabilities in Web Applications** 603
  Divya Muthukumaran, Dan O'Keeffe, Christian Priebe *(Imperial College London)*,
  David Eyers *(University of Otago),* Brian Shand *(NCRS, Public Health England),*
  Peter Pietzuch *(Imperial College London)*

- **Detecting and Exploiting Second Order Denial-of-Service Vulnerabilities in Web Applications** 616
  Oswaldo Olivo, Isil Dillig, Calvin Lin *(The University of Texas at Austin)*

- **Inlined Information Flow Monitoring for JavaScript** 629
  Andrey Chudnov, David A. Naumann *(Stevens Institute of Technology)*

Session 6C: Property-Preserving Encryption

- **Inference Attacks on Property-Preserving Encrypted Databases** 644
  Muhammad Naveed *(University of Illinois at Urbana Champaign),* Seny Kamara *(Microsoft Research),*
  Charles V. Wright *(Portland State University)*

- **Frequency-Hiding Order-Preserving Encryption** 656
  Florian Kerschbaum *(SAP)*

- **Leakage-Abuse Attacks Against Searchable Encryption** 668
  David Cash *(Rutgers University),* Paul Grubbs *(Skyhigh Networks Inc. & Cornell University),*
  Jason Perry *(Lewis University),* Thomas Ristenpart *(Cornell Tech)*

Session 7A: CryptoCurrency

- **Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions** 680
  Andrew Miller, Ahmed Kosba, Jonathan Katz *(University of Maryland),*
  Elaine Shi *(Cornell University)*

- **Tampering with the Delivery of Blocks and Transactions in Bitcoin** 692
  Arthur Gervais, Hubert Ritzdorf *(ETH Zurich),* Ghassan O. Karame *(NEC Laboratories Europe),*
  Srdjan Čapkun *(ETH Zurich)*

- **Demystifying Incentives in the Consensus Computer**..........706
  Loi Luu, Jason Teutsch, Raghav Kulkarni, Prateek Saxena *(National University of Singapore)*
- **Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges**..........720
  Gaby G. Dagher *(Concordia University),* Benedikt Bünz, Joseph Bonneau *(Stanford University),*
  Jeremy Clark *(Concordia University),* Dan Boneh *(Stanford University)*

Session 7B: Analyzing Obfuscated Code

- **Symbolic Execution of Obfuscated Code** 732
  Babak Yadegari, Saumya Debray *(University of Arizona)*
- **CoDisasm: Medium Scale Concatic Disassembly of Self-Modifying Binaries with Overlapping Instructions** 745
  Guillaume Bonfante *(Université de Lorraine, CNRS, INRIA),* Jose Fernandez *(Ecole Polytechnique de Montréal),*
  Jean-Yves Marion, Benjamin Rouxel, Fabrice Sabatier, Aurélien Thierry *(Université de Lorraine, CNRS, INRIA)*
- **LOOP: Logic-Oriented Opaque Predicate Detection in Obfuscated Binary Code**..........757
  Jiang Ming, Dongpeng Xu, Li Wang, Dinghao Wu *(The Pennsylvania State University)*
- **MalGene: Automatic Extraction of Malware Analysis Evasion Signature**..........769
  Dhilung Kirat, Giovanni Vigna *(University of California, Santa Barbara)*

Session 7C: Online Social Networks

- **Face/Off: Preventing Privacy Leakage From Photos in Social Networks** 781
  Panagiotis Ilia *(FORTH),* Iasonas Polakis *(Columbia University),* Elias Athanasopoulos *(FORTH),*
  Federico Maggi *(Politecnico di Milano),* Sotiris Ioannidis *(FORTH)*
- **CrowdTarget: Target-based Detection of Crowdturfing in Online Social Networks**..........793
  Jonghyuk Song, Sangho Lee, Jong Kim *(Pohang University of Science and Technology (POSTECH))*
- **Exploiting Temporal Dynamics in Sybil Defenses** 805
  Changchang Liu, Peng Gao *(Princeton University),* Matthew Wright *(University of Texas at Arlington),*
  Prateek Mittal *(Princeton University)*
- **Where's Wally? Precise User Discovery Attacks in Location Proximity Services**..........817
  Iasonas Polakis, George Argyros, Theofilos Petsios, Suphannee Sivakorn,
  Angelos D. Keromytis *(Columbia University)*

Session 8A: Outsourced Storage

- **Practicing Oblivious Access on Cloud Storage: the Gap, the Fallacy, and the New Way Forward**..........837
  Vincent Bindschaedler, Muhammad Naveed *(University of Illinois at Urbana-Champaign),*
  Xiaorui Pan *(Indiana University, Bloomington),* XiaoFeng Wang, Yan Huang *(Indiana University, Bloomington)*
- **Circuit ORAM: On Tightness of the Goldreich-Ostrovsky Lower Bound**..........850
  Xiao Shaun Wang *(University of Maryland),* T-H. Hubert Chan *(University of Hong Kong),*
  Elaine Shi *(Cornell)*
- **Constant Communication ORAM with Small Blocksize** 862
  Tarik Moataz *(Colorado State University & Telecom Bretagne, IMT),*
  Travis Mayberry *(United States Naval Academy),* Erik-Oliver Blass *(Airbus Group Innovations)*
- **Secure Deduplication of Encrypted Data without Additional Independent Servers**..........874
  Jian Liu *(Aalto University),* N. Asokan *(Aalto University and University of Helsinki),*
  Benny Pinkas *(Bar Ilan University)*
- **Transparent Data Deduplication in the Cloud**..........886
  Frederik Armknecht *(University of Mannheim),*
  Jens-Matthias Bohli, Ghassan O. Karame, Franck Youssef *(NEC Laboratories Europe)*

Session 8B: Control Flow Integrity

- **Control Jujutsu: On the Weaknesses of Fine-Grained Control Flow Integrity** 901
  Isaac Evans *(MIT Lincoln Laboratory),*
  Fan Long, Ulziibayar Otgonbaatar, Howard Shrobe, Martin Rinard *(Massachusetts Institute of Technology),*
  Hamed Okhravi *(MIT Lincoln Laboratory),* Stelios Sidiroglou-Douskos *(Massachusetts Institute of Technology)*

- **Per-Input Control-Flow Integrity** 914
  Ben Niu, Gang Tan *(Lehigh University)*

- **Practical Context-Sensitive CFI** 927
  Victor van der Veen, Dennis Andriesse, Enes Göktaş, Ben Gras, Lionel Sambuc *(VU University),*
  Asia Slowinska *(VU University / Lastline, Inc.),* Herbert Bos, Cristiano Giuffrida *(VU University)*

- **CCFI: Cryptographically Enforced Control Flow Integrity** 941
  Ali José Mashtizadeh, Andrea Bittau, Dan Boneh, David Mazières *(Stanford University)*

- **Losing Control: On the Effectiveness of Control-Flow Integrity under Stack Attacks** 952
  Mauro Conti *(University of Padua),* Stephen Crane *(University of California, Irvine),*
  Lucas Davi *(Technische Universität Darmstadt),* Michael Franz, Per Larsen *(University of California, Irvine)*,
  Marco Negro, Christopher Liebchen *(Technische Universität Darmstadt),*
  Mohaned Qunaibit *(University of California, Irvine),* Ahmad-Reza Sadeghi *(Technische Universität Darmstadt)*

Session 8C: Enhancing Trust

- **SEDA: Scalable Embedded Device Attestation** 964
  N. Asokan *(Aalto University and University of Helsinki),* Ferdinand Brasser *(Technische Universität Darmstadt),*
  Ahmad Ibrahim, Ahmad-Reza Sadeghi *(Technische Universität Darmstadt),* Matthias Schunter *(Intel Labs),*
  Gene Tsudik *(University of California, Irvine),* Christian Wachsmann *(Technische Universität Darmstadt)*

- **TrustOTP: Transforming Smartphones into Secure One-Time Password Tokens** 976
  He Sun *(College of William and Mary, Chinese Academy of Sciences & University of Chinese Academy of Sciences),*
  Kun Sun *(College of William and Mary),* Yuewu Wang, Jiwu Jing *(Chinese Academy of Sciences)*

- **Trusted Display on Untrusted Commodity Platforms** 989
  Miao Yu, Virgil D. Gligor, Zongwei Zhou *(Carnegie Mellon University)*

- **PyCRA: Physical Challenge-Response Authentication for Active Sensors Under Spoofing Attacks** 1004
  Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, Mani Srivastava
  (University of California, Los Angeles)

- **Clean Application Compartmentalization with SOAAP** 1016
  Khilan Gudka, Robert N.M. Watson *(University of Cambridge),* Jonathan Anderson *(Memorial University),*
  David Chisnall *(University of Cambridge),* Brooks Davis *(SRI International),*
  Ben Laurie *(Google UK Ltd.),* Ilias Marinos *(University of Cambridge),*
  Peter G. Neumann *(SRI International),* Alex Richardson *(University of Cambridge)*

Session 9A: Coding, Commitments, and Cipher Design

- **Falcon Codes: Fast, Authenticated LT Codes (Or: Making Rapid Tornadoes Unstoppable*)*** 1032
  Ari Juels *(Cornell Tech),* James Kelley *(NetApp, Inc.),* Roberto Tamassia *(Brown University),*
  Nikos Triandopoulos *(RSA Laboratories & Boston University)*

- **Fast Non-Malleable Commitments** 1048
  Hai Brenner *(IDC Herzliya),* Vipul Goyal *(Microsoft Research),*
  Silas Richelson *(University of California, Los Angeles),* Alon Rosen *(IDC Herzliya),*
  Margarita Vald *(Tel Aviv University)*

- **White-Box Cryptography Revisited: Space-Hard Ciphers** 1058
  Andrey Bogdanov *(Technical University of Denmark),* Takanori Isobe *(Sony Corporation)*
- **Lattice Basis Reduction Attack against Physically Unclonable Functions** 1070
  Fatemeh Ganji *(Technische Universität Berlin and Telekom Innovation Laboratories),*
  Juliane Krämer *(Technische Universität Darmstadt),*
  Jean-Pierre Seifert, Shahin Tajik *(Technische Universität Berlin and Telekom Innovation Laboratories)*

Session 9B: Security-Related Ecosystems

- **Drops for Stuff: An Analysis of Reshipping Mule Scams** 1081
  Shuang Hao, Kevin Borgolte *(University of California, Santa Barbara),*
  Nick Nikiforakis *(Stony Brook University),* Gianluca Stringhini *(University College London),*
  Manuel Egele *(Boston University),* Michael Eubanks *(Federal Bureau of Investigation),*
  Brian Krebs *(KrebsOnSecurity.com),* Giovanni Vigna *(University of California, Santa Barbara & Lastline Inc.)*
- **Android Root and its Providers: A Double-Edged Sword** 1093
  Hang Zhang, Dongdong She, Zhiyun Qian *(University of California, Riverside)*
- **An Empirical Study of Web Vulnerability Discovery Ecosystems** 1105
  Mingyi Zhao, Jens Grossklags, Peng Liu *(The Pennsylvania State University)*
- **The Dropper Effect: Insights into Malware Distribution with Downloader Graph Analytics** 1118
  Bum Jun Kwon, Jayanta Mondal *(University of Maryland),* Jiyong Jang *(IBM Research),*
  Leyla Bilge *(Symantec Research Labs),* Tudor Dumitras *(University of Maryland)*

Session 9C: Formal Methods Meet Cryptography

- **Equivalence-based Security for Querying Encrypted Databases: Theory and Application to Privacy Policy Audits** 1130
  Omar Chowdhury *(Purdue University),* Deepak Garg *(MPI-SWS),*
  Limin Jia, Anupam Datta *(Carnegie Mellon University)*
- **Automated Symbolic Proofs of Observational Equivalence** 1144
  David Basin, Jannik Dreier, Ralf Sasse *(ETH Zurich)*
- **Automated Proofs of Pairing-Based Cryptography** 1156
  Gilles Barthe *(IMDEA Software Institute),* Benjamin Grégoire *(INRIA),*
  Benedikt Schmidt *(IMDEA Software Institute)*
- **Moat: Verifying Confidentiality of Enclave Programs** 1169
  Rohit Sinha *(University of California, Berkeley),* Sriram Rajamani *(Microsoft Research),*
  Sanjit A. Seshia *(University of California, Berkeley),* Kapil Vaswani *(Microsoft Research)*

Session 10A: Key Exchange: Theory and Practice

- **On the Security of TLS 1.3 and QUIC Against Weaknesses in PKCS#1 v1.5 Encryption** 1185
  Tibor Jager, Jörg Schwenk, Juraj Somorovsky *(Horst Görtz Institute, Ruhr University Bochum)*
- **A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates** 1197
  Benjamin Dowling *(Queensland University of Technology),*
  Marc Fischlin, Felix Günther *(Technische Universität Darmstadt),*
  Douglas Stebila *(Queensland University of Technology)*
- **Deniable Key Exchanges for Secure Messaging** 1211
  Nik Unger, Ian Goldberg *(University of Waterloo)*
- **TOPAS: 2-Pass Key Exchange with Full Perfect Forward Secrecy and Optimal Communication Complexity** 1224
  Sven Schäge *(Ruhr-Universität Bochum)*

Session 10B: Mobile Device Attacks

- **From System Services Freezing to System Server Shutdown in Android: All You Need Is a Loop in an App** 1236
  Heqing Huang, Sencun Zhu *(The Pennsylvania State University),*
  Kai Chen *(Institute of Information Engineering, Chinese Academy of Sciences),*
  Peng Liu *(The Pennsylvania State University)*
- **Hare Hunting in the Wild Android: A Study on the Threat of Hanging Attribute References** 1248
  Yousra Aafer *(Syracuse University),* Nan Zhang *(Indiana University, Bloomington),*
  Zhongwen Zhang *(Chinese Academy of Sciences),* Xiao Zhang *(Syracuse University),*
  Kai Chen *(Chinese Academy of Sciences),* XiaoFeng Wang *(Indiana University, Bloomington),*
  Xiaoyong Zhou *(Samsung Research America),* Wenliang Du *(Syracuse University),*
  Michael Grace *(Samsung Research America)*
- **Perplexed Messengers from the Cloud: Automated Security Analysis of Push-Messaging Integrations** 1260
  Yangyi Chen *(Indiana University Bloomington),* Tongxin Li *(Peking University),*
  XiaoFeng Wang *(Indiana University Bloomington),*
  Kai Chen *(Indiana University Bloomington and Institute of Information Engineering, CAS),*
  Xinhui Han *(Peking University)*
- **When Good Becomes Evil: Keystroke Inference with Smartwatch** 1273
  Xiangyu Liu, Zhe Zhou, Wenrui Diao *(The Chinese University of Hong Kong),* Zhou Li *(ACM Member),*
  Kehuan Zhang *(The Chinese University of Hong Kong)*

Session 10C: Statistical Privacy

- **Differential Privacy with Bounded Priors: Reconciling Utility and Privacy in Genome-Wide Association Studies** 1286
  Florian Tramèr, Zhicong Huang, Jean-Pierre Hubaux *(Ecole Polytechnique Fédérale de Lausanne),*
  Erman Ayday *(Bilkent University)*
- **Protecting Locations with Differential Privacy under Temporal Correlations** 1298
  Yonghui Xiao, Li Xiong *(Emory University)*
- **Privacy-Preserving Deep Learning** 1310
  Reza Shokri *(University of Texas at Austin),* Vitaly Shmatikov *(Cornell Tech)*
- **Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures** 1322
  Matt Fredrikson *(Carnegie Mellon University),* Somesh Jha *(University of Wisconsin - Madison),*
  Thomas Ristenpart *(Cornell Tech)*

Session 11A: Privacy-Preserving Authentication

- **Group Signatures with Probabilistic Revocation: A Computationally-Scalable Approach for Providing Privacy-Preserving Authentication** 1334
  Vireshwar Kumar, He Li, Jung-Min (Jerry) Park *(Virginia Tech),* Kaigui Bian *(Peking University),*
  Yaling Yang *(Virginia Tech)*
- **Authenticating Privately over Public Wi-Fi Hotspots** 1346
  Aldo Cassola *(Northeastern University & Universidad San Francisco de Quito),*
  Erik-Oliver Blass *(Airbus Group Innovations & Northeastern University),*
  Guevara Noubir *(Northeastern University)*
- **SPRESSO: A Secure, Privacy-Respecting Single Sign-On System for the Web** 1358
  Daniel Fett, Ralf Küesters, Guido Schmitz *(University of Trier)*
- **Automating Fast and Secure Translations from Type-I to Type-III Pairing Schemes** 1370
  Joseph A. Akinyele, Christina Garman, Susan Hohenberger *(Johns Hopkins University)*

Session 11B: Web Attacks

- **The Clock is Still Ticking: Timing Attacks in the Modern Web** 1382
  Tom Van Goethem, Wouter Joosen *(KU Leuven),* Nick Nikiforakis *(Stony Brook University)*
- **Cross-Site Search Attacks** 1394
  Nethanel Gelernter, Amir Herzberg *(Bar Ilan University)*
- **The Spy in the Sandbox: Practical Cache Attacks in JavaScript and their Implications** 1406
  Yossef Oren, Vasileios P. Kemerlis, Simha Sethumadhavan, Angelos D. Keromytis *(Columbia University)*
- **From Facepalm to Brain Bender: Exploring Client-Side Cross-Site Scripting** 1419
  Ben Stock *(FAU Erlangen-Nuremberg),* Stephan Pfistner *(SAP SE),* Bernd Kaiser *(FAU Erlangen-Nuremberg),* Sebastian Lekies *(Ruhr-University Bochum),* Martin Johns *(SAP SE)*

Session 11C: Surveillance and Countermeasures

- **Mass-surveillance without the State: Strongly Undetectable Algorithm-Substitution Attacks** 1431
  Mihir Bellare, Joseph Jaeger, Daniel Kane *(University of California San Diego)*
- **HORNET: High-speed Onion Routing at the Network Layer** 1441
  Chen Chen *(Carnegie Mellon University & ETH Zürich),* Daniele E. Asoni, David Barrera *(ETH Zürich),* George Danezis *(University College London),* Adrain Perrig *(ETH Zürich)*
- **CARONTE: Detecting Location Leaks for Deanonymizing Tor Hidden Services** 1455
  Srdjan Matic *(Univerista degli Studi di Milano),* Platon Kotzias, Juan Caballero *(IMDEA Software Institute)*
- **(Un)linkable Pseudonyms for Governmental Databases** 1467
  Jan Camenisch, Anja Lehmann *(IBM Research - Zurich)*

Session 12A: Outsourcing Data and Computation

- **IntegriDB: Verifiable SQL for Outsourced Databases** 1480
  Yupeng Zhang, Jonathan Katz, Charalampos Papamanthou *(University of Maryland)*
- **A Domain-Specific Language for Low-Level Secure Multiparty Computation Protocols** 1492
  Peeter Laud *(Cybernetica AS),* Jaak Randmets *(Cybernetica AS and University of Tartu)*
- **Automated Synthesis of Optimized Circuits for Secure Computation** 1504
  Daniel Demmler, Ghada Dessouky *(TU Darmstadt),* Farinaz Koushanfar *(Rice University),* Ahmad-Reza Sadeghi, Thomas Schneider, Shaza Zeitouni *(TU Darmstadt)*
- **Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data** 1518
  Dario Catalano *(University of Catania),* Dario Fiore *(IMDEA Software Institute)*

Session 12B: Cloud, Web, and Authentication

- **Maneuvering Around Clouds: Bypassing Cloud-based Security Providers** 1530
  Thomas Vissers, Tom Van Goethem, Wouter Joosen *(KU Leuven),* Nick Nikiforakis *(Stony Brook University)*
- **The SICILIAN Defense: Signature-based Whitelisting of Web JavaScript** 1542
  Pratik Soni, Enrico Budianto, Prateek Saxena *(National University of Singapore)*
- **Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication** 1558
  Yan Li, Yingjiu Li, Qiang Yan, Hancong Kong, Robert H. Deng *(Singapore Management University)*

Session 12C: Side Channels

- **Observing and Preventing Leakage in MapReduce** 1570
  Olga Ohrimenko, Manuel Costa, Cédric Fournet, Christos Gkantsidis, Markulf Kohlweiss *(Microsoft Research),* Divya Sharma *(Carnegie Mellon University)*

- **Mitigating Storage Side Channels Using Statistical Privacy Mechanisms** 1582
  Qiuyu Xiao, Michael K. Reiter *(University of North Carolina),* Yinqian Zhang *(The Ohio State University)*
- **Nomad: Mitigating Arbitrary Cloud Side Channels via Provider-Assisted Migration** 1595
  Soo-Jin Moon, Vyas Sekar *(Carnegie Mellon University),* Michael K. Reiter *(University of North Carolina)*
- **Thwarting Memory Disclosure with Efficient Hypervisor-enforced Intra-domain Isolation** 1607
  Yutao Liu, Tianyu Zhou, Kexin Chen, Haibo Chen, Yubin Xia *(Shanghai Jiao Tong University)*

Demo & Poster Abstracts

- **DEMO: Action Recommendation for Cyber Resilience** 1620
  Luke Rodriguez, Darren Curtis, Sutanay Choudhury, Kiri Oler, Peter Nordquist *(Pacific Northwest National Lab),* Pin-Yu Chen *(University of Michigan Ann Arbor),* Indrajit Ray *(Colorado State University)*
- **POSTER: Secure Chat for the Masses? User-centered Security to the Rescue** 1623
  Ruba Abu-Salma, M. Angela Sasse *(University College London (UCL)),* Joseph Bonneau *(Stanford University/Electronic Frontier Foundation),* Matthew Smith *(University of Bonn)*
- **POSTER: In the Net of the Spider: Measuring the Anonymity-Impact of Network-level Adversaries Against Tor** 1626
  Michael Backes *(CISPA, Saarland University, MPI-SWS),* Simon Koch, Sebastian Meiser, Esfandiar Mohammadi, Christian Rossow *(CISPA, Saarland University)*
- **POSTER: Towards Compiler-Assisted Taint Tracking on the Android Runtime (ART*)*** ... 1629
  Michael Backes *(CISPA, Saarland University & MPI-SWS),* Oliver Schranz, Philipp von Styp-Rekowsky *(CISPA, Saarland University)*
- **POSTER: iPKI: Identity-based Private Key Infrastructure for Securing BGP Protocol** 1632
  Peixin Chen, Xiaofeng Wang, Yilun Wu, Jinshu Su, Huan Zhou *(National University of Defense Technology)*
- **POSTER: Mobile Device Identification by Leveraging Built-in Capacitive Signature** 1635
  Manh Huynh, Phuc Nguyen *(University of Colorado Denver),* Marco Gruteser *(Rutgers University),* Tam Vu *(University of Colorado Denver)*
- **POSTER: Implementing and Testing a Novel Chaotic Cryptosystem for Use in Small Satellites** 1638
  Samuel Jackson *(Oklahoma State University),* Scott Kerlin, Jeremy Straub *(University of North Dakota)*
- **POSTER: A Password-based Authentication by Splitting Roles of User Interface** 1641
  JungSeung Lee *(Samsung Electronics and Yonsei University),* Han Park, GyeongYong Bang, JooSeok Song *(Yonsei University)*
- **POSTER: Page Table Manipulation Attack** 1644
  JungSeung Lee *(Samsung Electronics and Yonsei University),* HyoungMin Ham, InHwan Kim, JooSeok Song *(Yonsei University)*
- **POSTER: Toward Energy-Wasting Misbehavior Detection Platform with Privacy Preservation in Building Energy Use** 1647
  Depeng Li *(University of Hawaii at Manoa),* Sachin Shetty *(Tennessee State University)*
- **POSTER: A Hardware Fingerprint Using GPU Core Frequency Variations** 1650
  Fengjun Li *(University of Kansas),* Xin Fu *(University of Houston),* Bo Luo *(University of Kansas)*
- **POSTER: The Popular Apps in Your Pocket Are Leaking Your Privacy** 1653
  Xing Liu, Wei Wang, Jiqiang Liu *(Beijing Jiaotong University)*
- **POSTER: PatchGen: Towards Automated Patch Detection and Generation for 1-Day Vulnerabilities** 1656
  Tianyue Luo, Chen Ni, Qing Han, Mutian Yang, Jingzheng Wu, Yanjun Wu *(Institute of Software, The Chinese Academy of Sciences)*

- **POSTER: Using Unit Testing to Detect Sanitization Flaws** 1659
  Mahmoud Mohammadi, Bill Chu, Heather Ritcher Lipford *(University of North Carolina at Charlotte)*
- **POSTER: PsychoRithm: A Framework for Studying How Human Traits Affect User Response to Security Situations** 1662
  Subhojeet Mukherjee, Sachini Weerawardhana, Chancey Dunn, Indrajit Ray, Adele Howe *(Colorado State University)*
- **POSTER: Dynamic Labelling for Analyzing Security Protocols** 1665
  N.V. Narendra Kumar *(Tata Institute of Fundamental Research),*
  R.K. Shyamasundar *(Indian Institute of Technology Bombay)*
- **POSTER: Computations on Encrypted Data in the Internet of Things Applications** 1668
  Laurynas Riliskis *(Stanford University),* Hossein Shafagh *(ETH Zurich),* Philip Levis *(Stanford University)*
- **POSTER: Detecting Malicious Web Pages based on Structural Similarity of Redirection Chains** 1671
  Toshiki Shibahara, Takeshi Yagi, Mitsuaki Akiyama, Yuta Takata, Takeshi Yada
  (NTT Secure Platform Labratories)
- **POSTER: WinOver Enterprise Dark Data** 1674
  Manish Shukla, Sumesh Manjunath, Rohit Saxena, Sutapa Mondal, Sachin Lodha *(TCS Innovation Labs)*
- **POSTER—A Logic Based Network Forensics Model for Evidence Analysis** 1677
  Anoop Singhal *(National Institute of Standards and Technology),* Changwei Liu *(George Mason University),*
  Duminda Wijesekara *(George Mason University and National Institute of Standards and Technology)*
- **POSTER: OFX: Enabling OpenFlow Extensions for Switch-Level Security Applications** 1678
  John Sonchack *(University of Pennsylvania),* Adam J. Aviv *(United States Naval Academy),*
  Eric Keller *(University of Colorado, Boulder),* Jonathan M. Smith *(University of Pennsylvania)*
- **POSTER: Blackboard-Based Electronic Warfare System** 1681
  Jeremy Straub *(University of North Dakota)*
- **POSTER: PRINCESS: A Secure Cloud File Storage System for Managing Data with Hierarchical Levels of Sensitivity** 1684
  Lihua Wang, Takuya Hayashi, Sachiko Kanamori, Atsushi Waseda, Ryo Nojima, Shiho Moriai *(NICT)*
- **POSTER: Pseudonymizing Client as a Privacy-Preserving Service: A Case Study of CDN** 1687
  Zheng Wang *(Qingdao University)*
- **POSTER: biTheft: Stealing Your Secrets by Bidirectional Covert Channel Communication with Zero-Permission Android Application** 1690
  Jingzheng Wu, Yanjun Wu, Mutian Yang, Zhifei Wu, Tianyue Luo,
  Yongji Wang *(Institute of Software, The Chinese Academy of Sciences)*
- **POSTER: Lightweight Streaming Authenticated Data Structures** 1693
  Chia-Mu Yu *(Yuan Ze University)*

Tutorial Abstracts

- **Fraud Detection through Graph-Based User Behavior Modeling** 1696
  Alex Beutel *(Carnegie Mellon University),* Leman Akoglu *(Stony Brook University),*
  Christos Faloutsos *(Carnegie Mellon University)*
- **Program Analysis for Mobile Application Integrity and Privacy Enforcement** 1698
  Marco Pistoia *(IBM T. J. Watson Research Center)*
- **Introduction to Cryptocurrencies** 1700
  Stefan Dziembowski *(University of Warsaw)*

Workshop Summaries

- **Workshop Summary of AISec'15 – 2015 Workshop on Artificial Intelligent and Security** 1702
  Christos Dimitrakakis, Aikaterini Mitrokotsa *(Chalmers University of Technology),*
  Arunesh Sinha *(University of Southern California)*

- **CCSW 2015: The 7th ACM Cloud Computing Security Workshop** 1703
  Florian Kerschbaum *(SAP),* Cristina Nita-Rotaru *(Purdue University),* Indrajit Ray *(Colorado State University)*

- **First Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC*):* Challenges and Research Directions** 1705
  Roshan K. Thomas *(The MITRE Corporation),* Alvaro A. Cardenas *(University of Texas at Dallas),*
  Rakesh B. Bobba *(Oregon State University)*

- **MIST 2015: 7th International Workshop on Managing Insider Security Threats** 1707
  Ilsun You *(Soon Chun Hyang University),* Elisa Bertino *(Purdue University)*

- **MTD 2015: Second ACM Workshop on Moving Target Defense** 1709
  George Cybenko *(Dartmouth College),* Dijiang Huang *(Arizona State University)*

- **SafeConfig 2015: Workshop on Automated Decision Making for Active Cyber Defense** 1711
  Ehab Al-Shaer *(University of North Carolina at Charlotte),*
  Christopher Oehmen *(Pacific Northwest National Laboratory),*
  Mohammad Ashiqur Rahman *(Tennessee Tech University)*

- **SPSM 2015: 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices** 1713
  David Lie *(University of Toronto),* Glenn Wurster *(BlackBerry)*

- **Fifth International Workshop on Trustworthy Embedded Devices (TrustED 2015*)*** 1715
  Jorge Guajardo *(Robert Bosch LLC),* Stefan Katzenbeisser *(TU Darmstadt)*

- **WISCS'15: The 2nd ACM Workshop on Information Sharing and Collaborative Security** 1717
  Tomas Sander *(Hewlett-Packard Laboratories),* Moti Yung *(Google Inc. and Columbia University)*

- **WPES 2015: The 14th Workshop on Privacy in the Electronic Society** 1719
  Nicholas Hopper *(University of Minnesota),* Rob Jansen *(U.S. Naval Research Laboratory)*

Author Index 1721

ACM CCS 2015 Conference Organization

General Chair:	Indrajit Ray *(Colorado State University, USA)*
Program Co-Chairs:	Ninghui Li *(Purdue University, USA)*
	Christopher Kruegel *(University of California, Santa Barbara, USA)*
Workshop Co-Chairs:	Xiaofeng Wang *(Indiana University, USA)*
	Kui Ren *(State University of New York, Buffalo, USA)*
Tutorial Co-Chairs:	James Joshi *(University of Pittsburgh, USA)*
	Rinku Dewri *(Denver University, USA)*
	Patrick Tague *(Carnegie Melon University, USA)*
Poster/Demo Co-Chairs:	Xinming (Simon) Ou *(University of South Florida, USA)*
	Sachin Shetty *(Tennessee State University, USA)*
	Anna Squicciarini *(Pennsylvania State University, USA)*
Proceedings Co-Chairs:	Feng Li *(Indiana University-Purdue University, USA)*
	Tarik Moataz *(Colorado State University, USA)*
Treasurer:	Yu Chen *(State University of New York, Binghamton, USA)*
Web Co-Chairs:	Chuan Yue *(Colorado School of Mines, USA)*
	Stacy Karas *(University of Colorado, Colorado Springs, USA)*
Student Travel Grant Co-Chairs	Indrakshi Ray *(Colorado State University, USA)*
	Hasan Takabi *(University of North Texas, USA)*
Registration Co-Chairs:	Alex Sprintson *(Texas A&M University, USA)*
	Mikhail Strizhov *(Colorado State University, USA)*
Publicity Co-Chairs:	Dongwan Shin *(New Mexico Tech., USA)*
	Dieudonne Mulamba *(Colorado State University, USA)*
Patron & Industry Outreach:	Christos Papadopoulos *(Colorado State University, USA)*
Local Arrangement Committee:	Ramki Thurimella *(Denver University, USA)*
	Edward Chow *(University of Colorado, Colorado Springs, USA)*

Steering Committee:

Somesh Jha (Chair) *(University of Wisconsin, Madison, USA)*
Helen Wang *(Microsoft Research, USA)*
Carl Landwehr *(George Washington University, USA)*
Giovanni Vigna *(University of California, Santa Barbara, USA)*
George Danezis *(University College London, UK)*
Trent Jaeger (SIGSAC Chair) *(Pennsylvania State University, USA)*
Stefan Savage *(University of California, San Diego, USA)*
David Basin *(ETH Zurich, Switzerland*)

Program Committee:

Gail Joon Ahn *(Arizona State University)*
Ehab Al-Shaer *(University of North Carolina at Charlotte)*
Manos Antonakakis *(Georgia Institute of Technology)*
Frederik Armknecht *(University of Mannheim, Germany)*
Michael Backes *(Saarland Univ. and MPI-SWS)*
Davide Balzarotti *(EURECOM)*
Gilles Barthe *(IMDEA Software Institute)*
Konstantin (Kosta) Beznosov *(University of British Columbia)*
Karthikeyan Bhargavan *(INRIA)*
Alex Biryukov *(University of Luxembourg)*
Marina Blanton *(University of Notre Dame)*
Joseph Bonneau *(Stanford University & EFF)*
Nikita Borisov *(University of Illinois at Urbana-Champaign)*
Kevin Butler *(University of Florida)*
Juan Caballero *(IMDEA Software Institute)*
Christian Cachin *(IBM Research)*
Srdjan Capkun *(ETH Zurich)*
Lorenzo Cavallaro *(Royal Holloway, University of London)*
Steve Checkoway *(Johns Hopkins University)*
Yan Chen *(Northwestern University)*
Omar Chowdhury *(Purdue University)*
George Danezis *(University College London)*
Alexander De Luca *(Google)*
Adam Doupe *(Arizona State University)*
Manuel Egele *(Boston University)*
William Enck *(North Carolina State University)*
Jose Fernandez *(École Polytechnique de Montreal)*
Dario Fiore *(IMDEA Software Institute)*
Pierre-Alain Fouque *(University Rennes)*
Michael Franz *(University of California, Irvine)*
Vinod Ganapathy *(Rutgers University)*
Deepak Garg *(MPI-SWS)*
Cristiano Giuffrida *(VU University, Amsterdam)*
Vipul Goyal *(Microsoft Research, India)*
J. Alex Halderman *(University of Michigan)*
William Harris *(Georgia Institute of Technology)*
Amir Herzberg *(Bar-Ilan University)*

Program Committee (Cont'd):

Thorsten Holz *(Ruhr-Universitaet Bochum)*
Amir Houmansadr *(University of Massachusetts, Amherst)*
Yan Huang *(Indiana University, Bloomington)*
Trent Jaeger *(Pennsylvania State University)*
Abhishek Jain *(Massachusetts Inst. of Technology and Boston University)*
Limin Jia *(Carnegie Mellon University)*
Hongxia Jin *(Samsung, USA)*
Brent Kang *(KAIST)*
Chris Kanich *(University of Illinois at Chicago)*
Stefan Katzenbeisser *(TU Darmstadt)*
Florian Kerschbaum *(SAP)*
Taesoo Kim *(Georgia Institute of Technology)*
Yongdae Kim *(KAIST)*
Engin Kirda *(Northeastern University)*
Ralf Kuesters *(University of Trier)*
Andrea Lanzi *(University of Milan)*
Peeter Laud *(Cybernetica AS)*
Wenke Lee *(Georgia Institute of Technology)*
Zhenkai Liang *(National University of Singapore)*
Benoit Libert *(ENS Lyon)*
Zhiqiang Lin *(University of Texas at Dallas)*
Yao Liu *(University of South Florida)*
Ben Livshits *(Microsoft Research)*
Long Lu *(Stony Brook University)*
Ashwin Machanavajjhala *(Duke University)*
Matteo Maffei *(Saarland University)*
Sarah Meiklejohn *(University College London)*
Prateek Mittal *(Princeton University)*
Ian Molloy *(IBM Research)*
Arvind Narayanan *(Princeton University)*
Nick Nikiforakis *(Stony Brook University)*
Hamed Okhravi *(MIT Lincoln Laboratory)*
Xinming Ou *(Kansas State University)*
Charalampos Papamanthou *(University of Maryland)*
Vern Paxson *(University of California, Berkley and ICSI)*
Mathias Payer *(Purdue University)*
Roberto Perdisci *(University of Georgia)*
Adrian Perrig *(ETH Zurich)*
Roberto Di Pietro *(Bell Labs, France)*
Benny Pinkas *(Bar Ilan University)*
Christina Poepper *(Ruhr-University Bochum)*
Bart Preneel *(KU Leuven and iMinds)*
Kui Ren *(University at Buffalo, SUNY)*
Konrad Rieck *(University of Goettingen)*
William Robertson *(Northeastern University)*
Andrei Sabelfeld *(Chalmers University of Technology)*

Program Committee (Cont'd):

Ahmad-Reza Sadeghi *(TU Darmstadt)*
Rei Safavi-Naini *(University of Calgary)*
Nitesh Saxena *(University of Alabama at Birmingham)*
Joerg Schwenk *(Ruhr-Universitaet Bochum)*
Hovav Shacham *(University of California, San Diego)*
Abhi Shelat *(University of Virginia)*
Elaine Shi *(University of Maryland)*
Kapil Singh *(IBM Research)*
Matthew Smith *(Universitaet Bonn)*
Francois-Xavier Standaert *(Universite Catholique de Louvain)*
Douglas Stebila *(Queensland University of Technology)*
Gianluca Stringhini *(University College London)*
Thorsten Strufe *(TU Dresden)*
Kun Sun *(College of William and Mary)*
Jakub Szefer *(Yale University)*
Gang Tan *(Lehigh University)*
Stefano Tessaro *(University of California, Santa Barbara)*
Mohit Tiwari *(University of Texas at Austin)*
Patrick Traynor *(University of Florida)*
Nikos Triandopoulos *(RSA Laboratories and Boston University)*
Mahesh Tripunitara *(University of Waterloo)*
Giovanni Vigna *(University of California, Santa Barbara)*
XiaoFeng Wang *(Indiana University)*
Zhi Wang *(Florida State University)*
Wenyuan Xu *(Zhejiang University)*
Guoliang Xue *(Arizona State University)*
Danfeng Yao *(Virginia Tech)*
Ting Yu *(Qatar Computing Research Institute)*
David Zage *(Sandia National Laboratories)*
Kehuan Zhang *(The Chinese University of Hong Kong)*
Xiangyu Zhang *(Purdue University)*
Yinqian Zhang *(Ohio State University)*
Yunlei Zhao *(Fudan University)*
Sheng Zhong *(Nanjing University)*
Haojin Zhu *(Shanghai Jiaotong University)*

ACM CCS 2015 Additional Reviewers

Michel Abdalla
Yasemin Acar
Steven Van Acker
David Adrian
Sadia Afroz
Shashank Agrawal
Mamunur Akand
Janaka Alawatugoda
Mashael Alsabah
Mohammed Alsaleh
Miguel Ambrona
Abhishek Anand
Prabhanjan Ananth
Elena Andreeva
Elli Androulaki
Zahid Anwar
Benny Applebaum
Daniel Arp
Giuseppe Ateniese
Christoph Bader
Shi Bai
Xiaolong Bai
Josep Balasch
Musard Balliu
Alexandru Bardas
Adam Bates
Martin Beck
Fabrice Benhamouda
Pascal Berrang
Sanjay Bhattacherjee
Vincent Bindschaedler
Bruno Blanchet
Jeremiah Blocki
Kevin Borgolte
Yazan Boshmaf
Raphael Bost
Kevin Bowers
Niklas Buescher
Sven Bugiel
Ahto Buldas
Adam Campbell
Frank Capobianco
Alvaro Cardenas
Angelo De Caro
Henry Carter
David Cash
Guilhem Castagnos
Dario Catalano
Nishanth Chandran
Jie Chen
Jing Chen
Rui Chen
Yilei Chen
Yizheng Chen
Yan Chen
Kai Chen
Yueqiang Cheng
Sherman Chow
Zheng Leong Chua
Simon Chung
Jeremy Clark
Ran Cohen
Baudoin Collard
Bart Coppens
Yann Le Corre
Veronique Cortier
Stephen Crane
Anupam Das
Santanu Dash
Sergej Dechand
Bart van Delft
Antoine Delignat-Lavaud
Jeroen Delvaux
Soteris Demetriou
Erik Derr
Julien Devigne
Claudia Diaz
Raushan Dilruba
Xinshu Dong
Benjamin Dowling
Evan Downing
Goran Doychev
Zakir Durumeric
Annie Edmunson
Fabienne Eigner
Steven Englehardt
Sascha Fahl
Ahmad Falakati
Matthieu Faou
Dennis Felsch
Daniel Fett
Chris Fletcher
Xinwen Fu
Benjamin Fuller
Marc Fyrbiak
Siddharth Garg
Behrad Garmany
Hugo Gascon
Paolo Gasti
Robert Gawlik
Xinyang Ge
Nethanel Gelernter
Yossi Gilad
Aris Gkoulalas-Divanis
Boru Gong
Matthew Green
Vincent Grosso
Tim Gueneysu
Felix Guenther
Florian Hahn
Samuel Haney
Shuang Hao
Daniel Hausknecht
Xi He
Daniel Hedin
Sven Heiberg
Mario Heiderich
Michael Herrmann
Matthew Hicks
Viet Tung Hoang
Dennis Hofheinz
Andrei Homescu
Justin Hsu
Hongxin Hu
Hong Hu
Yang Hu
Samee Zahur Al Islam
Angela Jaeschke
Tibor Jager
Yeongjin Jang
Kimmo Jarvinen
Mahavir Jhawar
Shouling Ji
Yaoqi Jia
Raul Pardo Jimenez
Yiming Jing
Rob Johnson
Zach Jorgensen
Marc Joye
Charanjit Jutla
Dina Kamel
Ghassan Karame
Nikolaos Karvelas
Aniket Kate
James Kelley
Yehonatan Kfir
Arman Khouzani
Dmitry Khovratovich
Dakshita Khurana
Panos Kintis
Nadim Kobeissi
Boris Koepf
Markulf Kohlweiss
Benjamin Kollenda
Deguang Kong
Philipp Koppe
Ahmed Kosba
Ios Kotsogiannis
Larry Koved
Ben Kreuter
Ivo Kubjas
Ranjit Kumaresan
Francois Labreche
Pascal Lafoucade
Junzuo Lai
Hanno Langweg
Per Larsen
Byoungyoung Lee
Yeonjoon Lee
Tancrede Lepoint
Chaz Lever
Fanny Lalonde Levesque

Allison Lewko
Ming Li
Mo Li
Shujun Li
Xiaolei Li
Yuping Li
Xiaopeng Li
Tongxin Li
Xiaojing Liao
Benjamin Liebe
Huijia Lin
Changchang Liu
Zhenming Liu
Kangjie Lu
Roel Maes
Jonas Magazinius
Bernardo Magri
Christian Mainka
Giulio Malavolta
Mark Manulis
Jian Mao
Antonio Marcedone
Daniel Masny
Sebastian Meiser
Sakis Meliopoulos
Wei Meng
Andrew Miller
Stanislav Miskovic
Vladislav Mladenov
Manar Mohamed
Ben Mood
Tal Moran
Louis-Philippe Morel
Pedro Moreno-Sanchez
Johannes Mueller
Martin Mulazzani
Yacin Nadji
Adwait Nadkarni
Muhammad Naveed
Kartik Nayak
Ajaya Neupane
Giang Nguyen
Marcus Niemitz
Ben Niu
Adam O'Neill
Gabriele Oligeri
Alina Oprea
Xiang Pan
Alisa Pankova
Dimitrios Papadopoulos
Stavros Papadopoulos
Davide Papini
Bryan Parno
Anat Paskin-Cherniavsky
Paul Pearce
Henning Perl
Leo Paul Perrin
Thomas Peters
Giuseppe Petracca
Duong-Hieu Phan
Phu Phung
Krzysztof Pietrzak
Antigoni Polychroniadou
Ivan Pryvalov
Pille Pullonen
Ivan Pustogarov
Chenxiong Qian
Zhan Qin
Zhenyang Qu
Max Rabkin
Willard Rafnsson
Carla Rafols
Somindu Ramanna
Vaibhav Rastogi
Daniel Rausch
Nisarg Raval
Bradley Reaves
Francesco Regazzoni
Tzachy Reinman
Ling Ren
Jan Reubold
Tamara Rezk
Mike Rosulek
Suman Saha
Sumanta Sarkar
Nolen Scaife
Guido Schmitz
Daniel Schoepe
Dominique Schroeder
Siamak Shahandashti
Yilin Shen
Maliheh Shirvanian
Babins Shrestha
Prakash Shrestha
Sander Siim
Mark Simkin
Juraj Somorovsky
Chengyu Song
Alessandro Sorniotti
Ron Steinfeld
Guillermo Suarez-Tangil
Yixin Sun
Yuqiong Sun
Sathya Chandran Sundaramurthy
Colleen Swanson
Somayeh Taheri
Nirupama Talele
Riivo Talviste
Qiang Tang
Ben Terner
Dave Tian
Michael Tschantz
Aleksei Udovenko
Matthias Vallentin
Nick Vasiloglou
Kapil Vaswani
Muthu Venkitasubramaniam
Daniele Venturi
Jorge Villar
Marko Vukolic
Sameer Wagh
Na Wang
Xiao Wang
Zhan Wang
Xiaolong Wang
Zhi Wang
Haoran Wang
Bogdan Warinschi
Hoeteck Wee
Jinpeng Wei
Sheng Wei
Fengguo Wei
Primal Wijesekera
Jan Willemson
Xitao Wen
Philipp Winter
Christian Wressnegger
Matthew Wright
Yanjing Wu
Eric Wustrow
Tao Xie
Luyi Xing
Jing Xu
Miao Xu
Khaled Yakdan
Chen Yan
Dejun Yang
Wei Yang
Shucheng Yu
Kan Yuan
Cheng Yueqiang
Insu Yun
Santiago Zanella-Beguelin
Mark Zhandry
Su Zhang
Tianwei Zhang
Yihua Zhang
Taimin Zhang
Nan Zhang
Xiaoyong Zhou
Yajin Zhou
Yuchen Zhou
Xinyan Zhou
Ralf Zimmermann
Saman Zonouz
Viviane Zwanger

ACM CCS 2015 Sponsor & Supporters

Sponsor

acm SIGSAC

Supporters

NSF

U.S.Army
Research Office

CISCO

SAP

Microsoft Research

Google

hp

IBM Research

Colorado State University

ASU