November 4–8, 2013
Berlin, Germany

Association for
Computing Machinery

Advancing Computing as a Science & Profession

CCS'13

The Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security

Sponsored by:

ACM SIGSAC

Supported by:

HGS, Army Research Office, BOSCH, SAP, NSF, Indiana University, CISCO, Intel, Google, Fraunhofer SIT, Heise Security, Microsoft Research, NXP, Kobil, Sirrix AG, Certgate, and IBM Research

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 © 2013 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: 978-1-4503-2477-9

Additional copies may be ordered prepaid from:

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

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

Printed in the USA

CCS 2013 General Chair’s Welcome

Information and communications security has become a fundamental element in our highly and globally computerized life. To tackle current and future security and privacy challenges adequately and globally, we need not only to advance research but also to bring together, from all over the world, researchers, developers and academics, as well as professionals from government agencies, research labs and corporate sectors.

The ACM Conference on Computer and Communications Security (CCS) is a leading forum, providing a highly suitable environment to conduct intellectual discussions and to exchange ideas. CCS is, in fact, the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association of Computing Machinery (ACM) and the oldest ACM conference in this field. Its reputation continues to grow and is reflected in its highly selective and prestigious technical program.

From 2002-2012, the number of paper submissions increased from about 150 to about 430. This year (2013), after more than a decade, CCS has moved to Europe/Germany. With 530 submissions we have witnessed the highest submission record in the history of CCS. Further, on the sponsorship side, CCS 2013 received over $125,000 funding support from various high-profile sources: The Army Research Office (ARO), The National Science Foundation (NSF), Bosch, Horst Görtz Stiftung (HGS), Fraunhofer SIT, SAP, Certgate, Google, Heise Security, Intel, Microsoft Research, NXP Semiconductors, IBM Research, Kobil and Sirrix AG. The Organizing Committee of CCS 2013 has put together an outstanding program that includes 105 papers (a new record), several keynote as well as invited speakers from academia, industry and government, 9 specialized pre- and post-conference workshops, 3 tutorials, 39 posters and demos, and one social event.

Given the above submission records causing an increased conference scale, organizing and setting up the program of CCS 2013 required a highly dedicated, committed and professional organizing committee, a strong technical program committee, and sponsoring decision makers who appreciate the high standards and impact of this flagship conference.

We are most grateful to the authors of the submitted papers (both to the main conference and to the workshops). We thank the technical program committee members and the program chairs as well as the external reviewers, who enabled a high quality review process. We thank the CCS 2013 Organizing Committee for selecting the workshops and tutorials on timely topics and cutting-edge technologies, and for the website design and maintenance, publications, publicity, local arrangements and registrations. Special acknowledgements go to the CCS Steering Committee, particularly to Prof. Elisa Bertino who strongly supported us with her advice. We thank the staff of the ACM for assisting us throughout the organization and publication process, the Center for Advanced Security Research Darmstadt (CASED) and the Fraunhofer SIT for providing their infrastructure and public relations. Last but not least, we would like to express our gratitude to our generous sponsors.

We wish you a pleasant stay in Berlin, a productive and highly utilized conference, and an exciting week at CCS 2013!

Ahmad-Reza Sadeghi
CCS 2013 General Chair
Technische Universität Darmstadt, Germany

CCS 2013 Program Chairs' Welcome

We are pleased to present to you the proceedings of the 2013 ACM Conference on Computer and Communications Security (CCS 2013), held in Berlin, Germany, November 4-8, 2013.

This year we received 530 submissions from 38 countries. This represents a record on at least two counts: it is both the largest number of submissions received by a computer security conference and the largest year-over-year submission increase (over 25%) to date. Remarkably, nearly half of the authors have professional affiliations in countries outside North America, with most in Europe and Asia-Pacific regions. A Program Committee comprising 82 experts from 16 countries as well as 310 external reviewers evaluated these submissions in the customary double-blind manner. At the end of the review process, 105 papers were selected for inclusion in the program, representing an acceptance rate of about 20%.

The review process was organized into three phases. After a first review phase, the authors of each paper were sent at least two preliminary reviews and 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. At the end of the second phase, 403 papers received at least 3 reviews, 120 received 4, and 7 received 5. The third phase included discussion of papers that remained under consideration at that stage, and after intensive debate, the final acceptance decisions were made.

As is typically the case with very competitive conferences, many of the papers that could not be included in the program contained interesting ideas. Some also included new research results worth reporting to the security community. For these reasons, we encouraged the authors of these papers to consider submitting their work to the specialized workshops associated with CCS, as appropriate. Other works that could not be accepted for the program, will surely see the light of day in other leading venues after suitable improvement. We hope that all authors benefitted from the feedback received from the CCS reviewers and that the review process has helped them improve their papers.

We are very grateful to the members of the Program Committee for their hard work, professionalism, and responsiveness under very tight deadlines. On average, each individual reviewed 21 papers, and nearly a third of the members volunteered to help shepherd accepted papers towards improved presentations. Most 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 2013 conference committee: the general chair, workshop co-chairs, tutorial co-chair, 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 all authors for submitting their work to CCS 2013 and to all attendees for their participation in technical discussion and debate. We hope that you find the program stimulating and enjoyable, and that your contributions will help further computer and communication security.

Virgil Gligor
ACM CCS '13 Program Chair
Carnegie Mellon University, USA

Moti Yung
ACM CCS '13 Program Chair
Google, USA

Table of Contents

CCS 2013 Conference Organization xvii

CCS 2013 Sponsor & Supporters xxiii

Session 1-A: Trusted Systems

- **A Security Framework for the Analysis and Design of Software Attestation** 1
  Frederik Armknecht *(Universität Mannheim),* Ahmad-Reza Sadeghi *(Technische Universität Darmstadt (CASED)),*
  Steffen Schulz *(Intel Corporation),* Christian Wachsmann *(Intel CRI-SC at TU Darmstadt)*
- **OASIS: On Achieving a Sanctuary for Integrity and Secrecy on Untrusted Platforms** 13
  Emmanuel Owusu *(Carnegie Mellon University),* Jorge Guajardo *(Robert Bosch LLC),*
  Jonathan McCune, Jim Newsome, Adrian Perrig, Amit Vasudevan *(Carnegie Mellon University)*
- **BIOS Chronomancy: Fixing the Core Root of Trust for Measurement** 25
  John Butterworth, Corey Kallenberg, Xeno Kovah, Amy Herzog *(The MITRE Corporation)*
- **Flexible and Scalable Digital Signatures in TPM 2.0** 37
  Liqun Chen *(Hewlett-Packard Labs),* Jiangtao Li *(Intel Corporation)*

Session 1-B: How Crypto Breaks

- **Rethinking SSL Development in an Appified World** 49
  Sascha Fahl, Marian Harbach, Henning Perl, Markus Koetter, Matthew Smith *(Leibniz University Hannover)*
- **Protocol Misidentification Made Easy with Format-Transforming Encryption** 61
  Kevin P. Dyer *(Portland State University),* Scott E. Coull *(RedJack, LLC.),*
  Thomas Ristenpart *(University of Wisconsin),* Thomas Shrimpton *(Portland State University)*
- **An Empirical Study of Cryptographic Misuse in Android Applications** 73
  Manuel Egele, David Brumley *(Carnegie Mellon University),*
  Yanick Fratantonio, Christopher Kruegel *(University of California, Santa Barbara)*
- **Detecting Stealthy, Distributed SSH Brute-Forcing** 85
  Mobin Javed *(University of California, Berkeley),*
  Vern Paxson *(University of California, Berkeley & International Computer Science Institute)*

Session 1-C: Malware

- **A Clinical Study of Risk Factors Related to Malware Infections** 97
  Fanny Lalonde Levésque, Jude Nsiempba, José M. Fernandez *(École Polytechnique de Montréal),*
  Sonia Chiasson, Anil Somayaji *(Carleton University)*
- **Delta: Automatic Identification of Unknown Web-Based Infection Campaigns** 109
  Kevin Borgolte, Christopher Kruegel, Giovanni Vigna *(University of California, Santa Barbara)*
- **Beheading Hydras: Performing Effective Botnet Takedowns** 121
  Yacin Nadji *(Georgia Institute of Technology),* Manos Antonakakis *(Damballa, Inc.),*
  Roberto Perdisci *(University of Georgia),* David Dagon, Wenke Lee *(Georgia Institute of Technology)*
- **Shady Paths: Leveraging Surfing Crowds to Detect Malicious Web Pages** 133
  Gianluca Stringhini, Christopher Kruegel, Giovanni Vigna *(University of California, Santa Barbara)*

Session 2-A: Passwords

- **Honeywords: Making Password-Cracking Detectable** 145
  Ari Juels *(RSA Laboratories),* Ronald L. Rivest *(Massachusetts Institute of Technology)*
- **Quantifying the Security of Graphical Passwords:**
  The Case of Android Unlock Patterns 161
  Sebastian Uellenbeck , Markus Dürmuth, Christopher Wolf, Thorsten Holz *(Ruhr-University Bochum)*

- **Measuring Password Guessability for an Entire University** 173
  Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
  (Carnegie Mellon University), Patrick Gage Kelley *(University of New Mexico),*
  Richard Shay, Blase Ur *(Carnegie Mellon University)*

- **SAuth: Protecting User Accounts from Password Database Leaks** 187
  Georgios Kontaxis, Elias Athanasopoulos *(Columbia University),*
  Georgios Portokalidis *(Stevens Institute of Technology),* Angelos D. Keromytis *(Columbia University)*

Session 2-B: Control & Information Flow

- **Monitor Integrity Protection with Space Efficiency and Separate Compilation** 199
  Ben Niu, Gang Tan *(Lehigh University)*

- **Relational Abstract Interpretation for the Verification of 2-Hypersafety Properties** 211
  Máté Kovács, Helmut Seidl *(Technische Universität München),* Bernd Finkbeiner *(Universität des Saarlandes)*

- **Formal Verification of Information Flow Security for a Simple ARM-Based Separation Kernel** 223
  Mads Dam, Roberto Guanciale, Narges Khakpour, Hamed Nemati *(KTH Royal Institute of Technology),*
  Oliver Schwarz *(SICS Swedish ICT)*

- **ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking** 235
  Kangkook Jee, Vasileios P. Kemerlis, Angelos D. Keromytis *(Columbia University),*
  Georgios Portokalidis *(Stevens Institute of Technology)*

Session 2-C: Storage Security

- **Multi-Cloud Oblivious Storage** 247
  Emil Stefanov *(University of California, Berkeley),* Elaine Shi *(University of Maryland)*

- **Policy-Based Secure Deletion** 259
  Christian Cachin, Kristiyan Haralambiev *(IBM Research - Zurich),*
  Hsu-Chun Hsiao *(Carnegie Mellon University),* Alessandro Sorniotti *(IBM Research - Zurich)*

- **Secure Data Deletion from Persistent Media** 271
  Joel Reardon, Hubert Ritzdorf , David Basin, Srdjan Capkun *(ETH Zurich)*

- **PoWerStore: Proofs of Writing for Efficient and Robust Storage** 285
  Dan Dobre, Ghassan O. Karame, Wenting Li *(NEC Labs Europe),* Matthias Majuntke *(Capgemini Deutschland),*
  Neeraj Suri *(TU Darmstadt),* Marko Vukolić *(EURECOM)*

Session 3-A: Oblivious RAM and Oblivious Computation

- **Path ORAM: An Extremely Simple Oblivious RAM Protocol** 299
  Emil Stefanov *(University of California, Berkeley),* Marten van Dijk *(University of Connecticut),*
  Elaine Shi *(University of Maryland),*
  Christopher Fletcher, Ling Ren, Xiangyao Yu, Srinivas Devadas *(Massachusetts Institute of Technology)*

- **PHANTOM: Practical Oblivious Computation in a Secure Processor** 311
  Martin Maas, Eric Love, Emil Stefanov *(University of California, Berkeley),* Mohit Tiwari *(University of Texas, Austin),*
  Elaine Shi *(University of Maryland, College Park),*
  Krste Asanović, John Kubiatowicz, Dawn Song *(University of California, Berkeley)*

- **Practical Dynamic Proofs of Retrievability** 325
  Elaine Shi *(University of Maryland),* Emil Stefanov *(University of California, Berkeley),*
  Charalampos Papamanthou *(University of Maryland)*

Session 3-B: Anonymous Channels

- **Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries** 337
  Aaron Johnson *(U.S. Naval Research Laboratory),* Chris Wacek *(Georgetown University),*
  Rob Jansen *(U.S. Naval Research Laboratory),* Micah Sherr *(Georgetown University),*
  Paul Syverson *(U.S. Naval Research Laboratory)*

- **PCTCP: Per-Circuit TCP-over-IPsec Transport for Anonymous Communication Overlay Networks** 349
  Mashael AlSabah *(Qatar University),* Ian Goldberg *(University of Waterloo)*

- **Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention** 361
  John Geddes, Max Schuchard, Nicholas Hopper *(University of Minnesota)*

Session 3-C: Protocol Analysis & Synthesis

- **An Analysis of the EMV Channel Establishment Protocol** 373
  Christina Brzuska *(Tel Aviv University),* Nigel P. Smart, Bogdan Warinschi, Gaven J. Watson *(University of Bristol)*
- **On the Security of TLS Renegotiation** 387
  Florian Giesen, Florian Kohlar *(Ruhr-Universität Bochum),* Douglas Stebila *(Queensland University of Technology)*
- **Using SMT Solvers to Automate Design Tasks for Encryption and Signature Schemes** 399
  Joseph A. Akinyele, Matthew Green, Susan Hohenberger *(Johns Hopkins University)*

Keynote Talk 1

- **The Science, Engineering and Business of Cyber Security** 411
  Ravi Sandhu *(University of Texas at San Antonio)*

Session 4-A: Network Security

- **AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks** 413
  Seungwon Shin *(Texas A&M University),* Vinod Yegneswaran, Phillip Porras *(SRI International),*
  Guofei Gu *(Texas A&M University)*
- **MinimaLT: Minimal-latency Networking Through Better Security** 425
  W. Michael Petullo *(United States Military Academy),* Xu Zhang, Jon A. Solworth *(University of Illinois at Chicago),*
  Daniel J. Bernstein *(University of Illinois at Chicago & TU Eindhoven),* Tanja Lange *(TU Eindhoven)*

Session 4-B: Critical Infrastructures

- **Impact of Integrity Attacks on Real-Time Pricing in Smart Grids** 439
  Rui Tan, Varun Badrinath Krishna *(Illinois at Singapore),*
  David K. Y. Yau *(University of Illinois at Singapore & Singapore University of Technology and Design),*
  Zbigniew Kalbarczyk *(University of Illinois at Urbana-Champaign)*
- **Configuration-based IDS for Advanced Metering Infrastructure** 451
  Muhammad Qasim Ali, Ehab Al-Shaer *(University of North Carolina Charlotte)*

Session 4-C: Attribute-based Encryption

- **Practical Constructions and New Proof Methods for Large Universe Attribute-Based Encryption** 463
  Yannis Rouselakis, Brent Waters *(The University of Texas at Austin)*
- **Blackbox Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on eBay** 475
  Zhen Liu *(Shanghai Jiao Tong University & City University of Hong Kong),*
  Zhenfu Cao *(Shanghai Jiao Tong University),* Duncan S. Wong *(City University of Hong Kong)*

Session 5-A: Programming Securely

- **Obfuscation Resilient Binary Code Reuse Through Trace-Oriented Programming** 487
  Junyuan Zeng, Yangchun Fu, Kenneth A. Miller, Zhiqiang Lin *(The University of Texas at Dallas),*
  Xiangyu Zhang, Dongyan Xu *(Purdue University)*
- **Chucky: Exposing Missing Checks in Source Code for Vulnerability Discovery** 499
  Fabian Yamaguchi *(University of Göttingen),* Christian Wressnegger *(idalab GmbH),*
  Hugo Gascon, Konrad Rieck *(University of Göttingen)*
- **Scheduling Black-box Mutational Fuzzing** 511
  Maverick Woo, Sang Kil Cha, Samantha Gottlieb, David Brumley *(Carnegie Mellon University)*

Session 5-B: Secure Multiparty Computation

- **Fast Two-Party Secure Computation with Minimal Assumptions** 523
  abhi shelat, Chih-hao Shen *(University of Virginia)*
- **More Efficient Oblivious Transfer and Extensions for Faster Secure Computation** 535
  Gilad Asharov, Yehuda Lindell *(Bar-Ilan University),* Thomas Schneider, Michael Zohner *(TU Darmstadt)*
- **An Architecture for Practical Actively Secure MPC with Dishonest Majority** 549
  Marcel Keller, Peter Scholl, Nigel P. Smart *(University of Bristol)*

Session 5-C: Formal Methods

- **Belief Semantics of Authorization Logic** 561
  Andrew K. Hirsch, Michael R. Clarkson *(George Washington University)*
- **Automatic Verification of Protocols with Lists of Unbounded Length** 573
  Bruno Blanchet, Miriam Paiola *(INRIA Paris-Rocquencourt)*
- **Relational Abstraction in Community-Based Secure Collaboration** 585
  Philip W. L. Fong, Pooya Mehregan *(University of Calgary),* Ram Krishnan *(University of Texas at San Antonio)*

Session 6-A: Mobile Security Issues

- **When Kids' Toys Breach Mobile Phone Security** 599
  Abdul Serwadda, Vir V. Phoha *(Louisiana Tech University)*
- **Vetting Undesirable Behaviors in Android Apps with Permission Use Analysis** 611
  Yuan Zhang, Min Yang, Bingquan Xu, Zhemin Yang *(Fudan University),* Guofei Gu *(Texas A&M University),*
  Peng Ning *(NC State University),* X. Sean Wang, Binyu Zang *(Fudan University)*
- **The Impact of Vendor Customizations on Android Security** 623
  Lei Wu, Michael Grace, Yajin Zhou, Chiachih Wu, Xuxian Jiang *(North Carolina State University)*
- **Unauthorized Origin Crossing on Mobile Platforms: Threats and Mitigation** 635
  Rui Wang *(Microsoft Research),* Luyi Xing, XiaoFeng Wang *(Indiana University),*
  Shuo Chen *(Microsoft Research)*

Session 6-B: Randomness

- **Security Analysis of Pseudo-Random Number Generators with Input: /dev/random is not Robust** 647
  Yevgeniy Dodis *(New York University),* David Pointcheval *(ENS-CNRS-INRIA),*
  Sylvain Ruhault *(ENS-CNRS-INRIA & Oppida, France),* Damien Vergnaud *(ENS-CNRS-INRIA),*
  Daniel Wichs *(Northeastern University)*
- **Predictability of Android OpenSSL's Pseudo Random Number Generator** 659
  Soo Hyeon Kim, Daewan Han *(The Attached Institute of ETRI),* Dong Hoon Lee *(Korea University)*
- **Delegatable Pseudorandom Functions and Applications** 669
  Aggelos Kiayias *(National and Kapodistrian University of Athens),* Stavros Papadopoulos *(HKUST),*
  Nikos Triandopoulos *(RSA Laboratories),* Thomas Zacharias *(National and Kapodistrian University of Athens)*
- **Ensuring High-Quality Randomness in Cryptographic Key Generation** 685
  Henry Corrigan-Gibbs, Wendy Mu, Dan Boneh *(Stanford University),* Bryan Ford *(Yale University)*

Session 6-C: Hardware Security

- **FANCI: Identification of Stealthy Malicious Logic Using Boolean Functional Analysis** 697
  Adam Waksman, Matthew Suozzo, Simha Sethumadhavan *(Columbia University)*
- **Security Analysis of Integrated Circuit Camouflaging** 709
  Jeyavijayan Rajendran, Michael Sam *(Polytechnic Institute of NYU),*
  Ozgur Sinanoglu *(New York University - Abu Dhabi),* Ramesh Karri *(Polytechnic Institute of NYU)*

- **Low-Fat Pointers: Compact Encoding and Efficient Gate-Level Implementation of Fat Pointers for Spatial Safety and Capability-Based Security** 721
Albert Kwon, Udit Dhawan, Jonathan M. Smith *(University of Pennsylvania),* Thomas F. Knight, Jr. *(Gingko Bioworks),* André DeHon *(University of Pennsylvania)*
- **Breaking and Entering Through the Silicon** 733
Clemens Helfmeier, Dmitry Nedospasov *(Berlin University of Technology),* Christopher Tarnovsky *(IOActive),* Jan Krissler *(Technische Universität Berlin),* Christian Boit, Jean-Pierre Seifert *(Berlin University of Technology)*

Session 7-A: Web Attacks

- **Polyglots: Crossing Origins by Crossing Formats** 753
Jonas Magazinius *(Chalmers University of Technology),* Billy K. Rios *(Cylance, Inc.),* Andrei Sabelfeld *(Chalmers University of Technology)*
- **ViceROI: Catching Click-Spam in Search Ad Networks** 765
Vacha Dave *(UC San Diego),* Saikat Guha *(Microsoft Research India),* Yin Zhang *(University of Texas at Austin)*
- **mXSS Attacks: Attacking Well-Secured Web-Applications by Using innerHTML Mutations** 777
Mario Heiderich, Jöerg Schwenk, Tilman Frosch *(Ruhr-University Bochum),* Jonas Magazinius *(Chalmers University of Technology),* Edward Z. Yang *(Stanford University)*

Session 7-B: Privacy-Preserving Protocols

- **When Private Set Intersection Meets Big Data: An Efficient and Scalable Protocol** 789
Changyu Dong *(University of Strathclyde),* Liqun Chen *(Hewlett-Packard Laboratories),* Zikai Wen *(University of Strathclyde)*
- **Privacy-Preserving Matrix Factorization** 801
Valeria Nikolaenko *(Stanford University),* Stratis Ioannidis, Udi Weinsberg, Marc Joye, Nina Taft *(Technicolor),* Dan Boneh *(Stanford University)*
- **PICCO: A General-Purpose Compiler for Private Distributed Computation** 813
Yihua Zhang, Aaron Steele, Marina Blanton *(University of Notre Dame)*

Session 7-C: Systems' Attack Mitigation

- **Düppel: Retrofitting Commodity Operating Systems to Mitigate Cache Side Channels in the Cloud** 827
Yinqian Zhang, Michael K. Reiter *(University of North Carolina at Chapel Hill)*
- **Tappan Zee (North) Bridge: Mining Memory Accesses for Introspection** 839
Brendan Dolan-Gavitt *(Georgia Institute of Technology),* Tim Leek, Josh Hodosh *(Massachusetts Institute of Technology),* Wenke Lee *(Georgia Institute of Technology)*
- **Towards Reducing the Attack Surface of Software Backdoors** 851
Felix Schuster, Thorsten Holz *(Ruhr-University Bochum)*

Session 8-A: Secure Outsourcing Protocols

- **Verifiable Delegation of Computation on Outsourced Data** 863
Michael Backes *(Saarland University & MPI-SWS),* Dario Fiore *(MPI-SWS),* Raphael M. Reischuk *(Saarland University)*
- **Outsourced Symmetric Private Information Retrieval** 875
Stanislaw Jarecki *(University of California, Irvine),* Charanjit Jutla, Hugo Krawczyk *(IBM Research),* Marcel Rosu *(University of California, Irvine),* Michael Steiner *(IBM Research)*

Session 8-B: Privacy Models

- **Membership Privacy: A Unifying Framework for Privacy Definitions** 889
Ninghui Li, Wahbeh Qardaji, Dong Su, Yi Wu, Weining Yang *(Purdue University)*
- **Geo-Indistinguishability: Differential Privacy for Location-Based Systems** 901
Miguel E. Andrés *(École Polytechnique),* Nicolás E. Bordenabe *(INRIA & École Polytechnique),* Konstantinos Chatzikokolakis *(CNRS & École Polytechnique),* Catuscia Palamidessi *(INRIA & École Polytechnique),*

Session 8-C: Be Aware & Beware

- **Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education** 915
  Tamara Denning, Adam Lerner *(University of Washington),* Adam Shostack *(Unaffiliated),*
  Tadayoshi Kohno *(University of Washington)*

- **Security Analysis of a Widely Deployed Locking System** 929
  Michael Weiner *(Technische Universität München),* Maurice Massar *(Technische Universität Kaiserslautern),*
  Erik Tews, Dennis Giese *(Technische Universität Darmstadt),*
  Wolfgang Wieser *(Ludwig-Maximilians-Universität München)*

Keynote Talk 2

- **The Cyber Arms Race** 941
  Mikko Hypponen *(F-Secure)*

Session 9-A: Crypto Tools

- **How to Keep a Secret: Leakage Deterring Public-key Cryptosystems** 943
  Aggelos Kiayias *(National and Kapodistrian University of Athens),*
  Qiang Tang *(National and Kapodistrian University of Athens & University of Connecticut)*

- **Zero-Knowledge Using Garbled Circuits: How to Prove Non-Algebraic Statements Efficiently** 955
  Marek Jawurek, Florian Kerschbaum *(SAP),* Claudio Orlandi *(Aarhus University)*

- **Elligator: Elliptic-Curve Points Indistinguishable from Uniform Random Strings** 967
  Daniel J. Bernstein *(University of Illinois at Chicago),* Mike Hamburg *(Rambus),*
  Anna Krasnova *(Radboud University Nijmegen),* Tanja Lange *(Technische Universiteit Eindhoven)*

Session 9-B: Audit & Code Randomization

- **ASIST: Architectural Support for Instruction Set Randomization** 981
  Antonis Papadogiannakis, Laertis Loutsis, Vassilis Papaefstathiou, Sotiris Ioannidis *(Hellas)*

- **librando: Transparent Code Randomization for Just-in-Time Compilers** 993
  Andrei Homescu, Stefan Brunthaler, Per Larsen, Michael Franz *(University of California, Irvine)*

- **LogGC: Garbage Collecting Audit Log** 1005
  Kyu Hyung Lee, Xiangyu Zhang, Dongyan Xu *(Purdue University)*

Session 9-C: Mobile Privacy

- **Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources** 1017
  Xiaoyong Zhou *(Indiana University, Bloomington),*
  Soteris Demetriou, Dongjing He, Muhammad Naveed *(University of Illinois at Urbana-Champaign),*
  Xiaorui Pan, XiaoFeng Wang *(Indiana University, Bloomington),*
  Carl A. Gunter, Klara Nahrstedt *(University of Illinois at Urbana-Champaign)*

- **Preventing Accidental Data Disclosure in Modern Operating Systems** 1029
  Adwait Nadkarni, William Enck *(North Carolina State University)*

- **AppIntent: Analyzing Sensitive Data Transmission in Android for Privacy Leakage Detection** 1043
  Zhemin Yang, Min Yang, Yuan Zhang *(Fudan University),* Guofei Gu *(Texas A&M University),*
  Peng Ning *(NC State University),* X. Sean Wang *(Fudan University)*

Session 10-A: Graphics, Vision & Security

- **Cross-Origin Pixel Stealing: Timing Attacks Using CSS Filters** 1055
  Robert Kotcher, Yutong Pei, Pranjal Jumde, Collin Jackson *(Carnegie Mellon University)*

- **Seeing Double: Reconstructing Obscured Typed Input from Repeated Compromising Reflections** 1063
  Yi Xu, Jared Heinly, Andrew M. White, Fabian Monrose, Jan-Michael Frahm
  (University of North Carolina at Chapel Hill)

- **The Robustness of Hollow CAPTCHAs** 1075
  Haichang Gao, Wei Wang, Jiao Qi, Xuqin Wang, Xiyang Liu *(Xidian University)*, Jeff Yan *(Newcastle University)*

Session 10-B: Authentication

- **Anonymous Credentials Light** 1087
  Foteini Baldimtsi, Anna Lysyanskaya *(Brown University)*

- **Heart-to-Heart (H2H): Authentication for Implanted Medical Devices** 1099
  Masoud Rostami *(Rice University)*, Ari Juels *(RSA Laboratories)*, Farinaz Koushanfar *(Rice University)*

- **OAKE: A New Family of Implicitly Authenticated Diffie-Hellman Protocols** 1113
  Andrew Chi-Chih Yao *(Tsinghua University)*, Yunlei Zhao *(Fudan University)*

Session 10-C: Privacy Issues

- **FPDetective: Dusting the Web for Fingerprinters** 1129
  Gunes Acar *(KU Leuven)*, Marc Juarez *(KU Leuven & IIIA-CSIC)*, Nick Nikiforakis, Claudia Diaz *(KU Leuven)*,
  Seda Gürses *(KU Leuven & New York University)*, Frank Piessens, Bart Preneel *(KU Leuven)*

- **Addressing the Concerns of the Lacks Family: Quantification of Kin Genomic Privacy** 1141
  Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux *(École Polytechnique Fédérale de Lausanne)*,
  Amalio Telenti *(University Hospital of Lausanne)*

- **Hang with Your Buddies to Resist Intersection Attacks** 1153
  David Isaac Wolinsky, Ewa Syta, Bryan Ford *(Yale University)*

Session 11-A: Web and Code Security

- **Content-Based Isolation: Rethinking Isolation Policy Design on Client Systems** 1167
  Alexander Moshchuk, Helen J. Wang *(Microsoft Research)*, Yunxin Liu *(Microsoft Research Asia)*

- **Diglossia: Detecting Code Injection Attacks with Precision and Efficiency** 1181
  Sooel Son *(The University of Texas at Austin)*,
  Kathryn S. McKinley *(The University of Texas at Austin & Microsoft Research)*,
  Vitaly Shmatikov *(The University of Texas at Austin)*

- **25 Million Flows Later - Large-Scale Detection of DOM-based XSS** 1193
  Sebastian Lekies *(SAP AG)*, Ben Stock *(Friedrich-Alexander-University Erlangen-Nuremberg)*,
  Martin Johns *(SAP AG)*

- **deDacota: Toward Preventing Server-Side XSS Via Automatic Code and Data Separation** 1205
  Adam Doupé *(University of California, Santa Barbara)*,
  Weidong Cui, Mariusz H. Jakubowski, Marcus Peinado *(Microsoft Research)*,
  Christopher Kruegel, Giovanni Vigna *(University of California, Santa Barbara)*

Session 11-B: Crypto Symbolic Analysis

- **Certified Computer-Aided Cryptography: Efficient Provably Secure Machine Code from High-Level Implementations** 1217
  José Bacelar Almeida, Manuel Barbosa *(HasLab & Universidade do Minho)*,
  Gilles Barthe, François Dupressoir *(IMDEA Software Institute)*

- **Computationally Complete Symbolic Attacker and Key Exchange** 1231
  Gergei Bana *(INRIA, Paris),* Koji Hasebe *(University of Tsukuba),* Mitsuhiro Okada *(Keio University)*
- **Fully Automated Analysis of Padding-Based Encryption in the Computational Model** 1247
  Gilles Barthe, Juan Manuel Crespo *(IMDEA Software Institute),* Benjamin Grégoire *(INRIA Sophia Antipolis),*
  César Kunz *(IMDEA Software Institute),* Yassine Lakhnech *(U. de Grenoble & VERIMAG),*
  Benedikt Schmidt *(IMDEA Software Institute),* Santiago Zanella-Béguelin *(Microsoft Research)*
- **Deduction Soundness: Prove One, Get Five for Free** 1261
  Florian Böhl *(KIT),* Véronique Cortier *(CNRS, Loria),* Bogdan Warinschi *(University of Bristol)*

Session 11-C: Security/Cryptographic Utilities

- **Efficient Targeted Key Subset Retrieval in Fractal Hash Sequences** 1273
  Kelsey Cairns, Thoshitha Gamage, Carl Hauser *(Washington State University)*
- **HIFS: History Independence for File Systems** 1285
  Sumeet Bajaj, Radu Sion *(Stony Brook University)*
- **AUTOCRYPT: Enabling Homomorphic Computation on Servers to Protect Sensitive Web Content** 1297
  Shruti Tople, Shweta Shinde, Zhaofeng Chen, Prateek Saxena *(National University of Singapore)*
- **Protecting Sensitive Web Content from Client-Side Vulnerabilities with CRYPTONS** 1311
  Xinshu Dong *(National University of Singapore),* Zhaofeng Chen *(Peking University),*
  Hossein Siadati *(Polytechnic Institute of New York University),*
  Shruti Tople, Prateek Saxena, Zhenkai Liang *(National University of Singapore)*

Demonstration Presentations

- **DEMO: Adjustably Encrypted In-Memory Column-Store** 1325
  Florian Kerschbaum, Patrick Grofig, Isabelle Hang, Martin Härterich, Mathias Kohler, Andreas Schaad,
  Axel Schröpfer, Walter Tighzert *(SAP)*
- **DEMO: Demonstrating a Trust Framework for Evaluating GNSS Signal Integrity** 1329
  Xihui Chen *(University of Luxembourg),* Carlo Harpes *(itrust consulting, Luxembourg),*
  Gabriele Lenzini *(University of Luxembourg),* Miguel Martins *(itrust consulting, Luxembourg),*
  Sjouke Mauw, Jun Pang *(University of Luxembourg)*
- **DEMO: Inherent PUFs and Secure PRNGs on Commercial Off-the-Shelf Microcontrollers** 1333
  Anthony Van Herrewege *(KU Leuven),* André Schaller, Stefan Katzenbeisser *(TU Darmstadt),*
  Ingrid Verbauwhede *(KU Leuven)*
- **DEMO: An IDS Framework for Internet of Things Empowered By 6LoWPAN** 1337
  Prabhakaran Kasinathan, Gianfranco Costamagna, Hussein Khaleel, Claudio Pastrone, Maurizio A. Spirito
  (Istituto Superiore Mario Boella)
- **DEMO: Secure and Customizable Web Development in the SAFE Activation Framework** 1341
  Raphael M. Reischuk, Florian Schröder *(Saarland University),* Johannes Gehrke *(Cornell University)*
- **DEMO: Enabling Trusted Stores for Android** 1345
  Yury Zhauniarovich, Olga Gadyatskaya, Bruno Crispo *(University of Trento)*
- **DEMO: Gradiant Asymmetric Encryption and Verification Systems Based on Handwritten Signature** 1349
  Enrique Argones Rúa, Francisco Javier García Salomón, Luis Pérez-Freire
  (GRADIANT - Galician R&D Center in Advanced Telecommunications)
- **DEMO: On the Real-Time Masking of the Sound of Credit Cards Using Hot Patching** 1351
  Manish Shukla, Purushotam Radadia, Shirish Karande, Sachin Lodha *(TRDDC)*

Poster Presentations

- **POSTER: Critique of the CISSP Common Body of Knowledge of Cryptography** 1355
  Stephan Neuhaus *(ETH Zurich),* Gabriela Gheorghe *(University of Luxembourg)*

- **POSTER: Preserving Privacy and Accountability for Personal Devices** 1359
  Gabriela Gheorghe *(University of Luxembourg),* Stephan Neuhaus *(Eidgenössische Technische Hochschule)*
- **POSTER: Caching Oblivious Memory Access: An Extension to the HCRYPT Virtual Machine** 1363
  Michael Brenner, Matthew Smith *(Gottfried Wilhelm Leibniz Universität)*
- **POSTER: Data Quality Evaluation: Integrating Security and Accuracy** 1367
  Leon Reznik *(Rochester Institute of Technology),* Elisa Bertino *(Purdue University)*
- **POSTER: Graphical Password Using Object-Based Image Ranking** 1371
  Cuong Xuan Nguyen, Hung-Hsuan Huang , Kyoji Kawagoe *(Ritsumeikan University)*
- **POSTER: A Semantic-Aware Approach to Reasoning about Network Traffic Relations** 1375
  Hao Zhang, Danfeng Daphne Yao, Naren Ramakrishnan *(Virginia Tech)*
- **POSTER: Detecting Malware Through Temporal Function-Based Features** 1379
  Eitan Menahem, Asaf Shabtai, Adi Lavhar *(Ben-Gurion University of the Negev)*
- **POSTER: Event-Based Isolation of Critical Data in the Cloud** 1383
  Sebastian Biedermann, Stefan Katzenbeisser *(Technische Universität Darmstadt)*
- **POSTER: BotFlex: A Community-Driven Tool for Botnet Detection** 1387
  Sheharbano Khattak *(Independent Researcher),*
  Zaafar Ahmed, Affan Syed *(SysNet, National University of Computer & Emerging Sciences),*
  Syed Ali Khayam *(PLUMgrid, Inc.)*
- **POSTER: Signal Anomaly Based Attack Detection in Wireless Sensor Networks** 1391
  Jeton Bacaj, Leon Reznik *(Rochester Institute of Technology)*
- **POSTER: Enhanced Embedded Device Security by Combining Hardware-Based Trust Mechanisms** 1395
  Martin Schramm, Karl Leidl, Andreas Grzemba *(University of Applied Sciences Deggendorf),*
  Nicolai Kuntze *(Fraunhofer SIT)*
- **POSTER: On the Anonymity of Israel's General Elections** 1399
  Tomer Ashur, Orr Dunkelman *(University of Haifa)*
- **POSTER: Secure Authentication from Facial Attributes with No Privacy Loss** 1403
  Orr Dunkelman, Margarita Osadchy, Mahmood Sharif *(University of Haifa)*
- **POSTER: Performance Signatures of Mobile Phone Browsers** 1407
  Bilal Shebaro, Di Jin, Elisa Bertino *(Purdue University)*
- **POSTER: A New Framework Against Privilege Escalation Attacks on Android** 1411
  Wenming Zhou *(Xidian University),* Yuqing Zhang *(UCAS),* Xuefeng Liu *(Xidian University)*
- **POSTER—Triplex: Verifying Data Minimisation in Communication Systems** 1415
  Meilof Veeningen, Mayla Brusò, Jerry den Hartog, Nicola Zannone *(Eindhoven University of Technology)*
- **POSTER: SHAMROCK: Self Contained Cryptography and Key Management Processor** 1419
  Daniil Utin, Roger Khazan, Joshua Kramer, Michael Vai, David Whelihan *(Massachusetts Institute of Technology)*
- **POSTER: Trend of Online Flash XSS Vulnerabilities** 1421
  Qixu Liu, Yuqing Zhang *(University of Chinese Academy of Sciences),* Huan Yang *(Xidian University)*
- **POSTER: Cross-Platform Malware: Write Once, Infect Everywhere** 1425
  Martina Lindorfer, Matthias Neumayr *(Vienna University of Technology),*
  Juan Caballero *(IMDEA Software Institute),* Christian Platzer *(Vienna University of Technology)*
- **POSTER: Introducing Pathogen: A Real-Time Virtual Machine Introspection Framework** 1429
  Anthony Roberts, Richard McClatchey, Saad Liaquat *(University of the West of England),*
  Nigel Edwards, Mike Wray *(Hewlett-Packard Laboratories)*
- **POSTER — PnP: Improving Web Browsing Performance Over Tor Using Web Resource Prefetch-and-Push** 1433
  Giang T. K. Nguyen, Xun Gong, Anupam Das, Nikita Borisov *(University of Illinois at Urbana-Champaign)*

- **POSTER: Sniffing and Propagating Malwares through WPAD Deception in LANs** 1437
  Li Dan *(Beijing University of Posts and Telecommunications & Chinese Academy of Science),*
  Chaoge Liu *(Chinese Academy of Sciences),* Xu Cui *(China Academy of Aerospace Aerodynamics),*
  Xiang Cui *(Chinese Academy of Sciences)*
- **POSTER: A Footprint of Third-Party Tracking on Mobile Web** 1441
  Ashar Javed *(Chair of Network & Data Security, Ruhr University Bochum)*
- **POSTER: Dr. Watson Provides Data for Post-Breach Analysis** 1445
  Wasim Ahmad Bhat, S. M. K. Quadri *(University of Kashmir)*
- **POSTER: Reflected Attacks Abusing Honeypots** 1449
  Martin Husák, Martin Vizváry *(Masaryk University)*
- **POSTER — TouchCtrl: Fine-Grained Access Control for Collaborative Environments** 1453
  Benjamin Güldenring, Volker Roth *(Freie Universität Berlin)*
- **POSTER — CRYPTSERVER: Strong Data Protection in Commodity LAMP Servers** 1457
  Zhaofeng Chen *(Peking University),* Xinshu Dong, Prateek Saxena, Zhenkai Liang *(National University of Singapore)*
- **POSTER: Identity-Based Steganography and Its Applications to Censorship Resistance** 1461
  Tim Ruffing, Jonas Schneider, Aniket Kate *(Saarland University)*
- **POSTER — Sechduler: A Security-Aware Kernel Scheduler** 1465
  Parisa Haghani *(University of Illinois at Urbana-Champaign),* Saman Zonouz *(University of Miami)*
- **POSTER: Passwords on Flexible Display Devices** 1469
  Sana Maqsood, Sonia Chiasson, Audrey Girouard *(Carleton University)*
- **POSTER: Revisiting Anomaly Detection System Design Philosophy** 1473
  Ayesha Binte Ashfaq *(National University of Sciences and Technology),*
  Muhammad Qasim Ali, Ehab Al-Shaer *(University of North Carolina Charlotte),* Syed Ali Khayam *(PLUMgrid Inc.)*

Workshop Summaries

- **12th Workshop on Privacy in the Electronic Society (WPES 2013)** 1477
  Sara Foresti *(Università degli Studi di Milano)*
- **Third International Workshop on Trustworthy Embedded Devices (TrustED 2013)** 1479
  Frederik Armknecht *(Universität Mannheim),*
  Jean-Pierre Seifert *(Technische Universität Berlin & Deutsche Telekom Laboratories)*
- **CyCAR'2013: First International Academic Workshop on Security, Privacy and Dependability for CyberVehicles** 1481
  Arslan Munir, Farinaz Koushanfar *(Rice University),* Hervé Seudié *(Robert Bosch GmbH),*
  Ahmad-Reza Sadeghi *(Intel CRISC & TU Darmstadt)*
- **Summary/Overview for Artificial Intelligence and Security (AISec'13)** 1483
  Blaine Nelson *(University of Potsdam),* Christos Dimitrakakis *(Chalmers University)*
  Elaine Shi *(University of Maryland)*
- **The First Workshop on Language Support for Privacy-Enhancing Technologies (PETShop'13)** 1485
  Martin Franz *(Deutsche Bank),* Andreas Holzer *(Vienna University of Technology),*
  Rupak Majumdar *(Max Planck Institute for Software Systems),* Bryan Parno *(Microsoft Research),*
  Helmut Veith *(Vienna University of Technology)*
- **Fifth ACM Cloud Computing Security Workshop (CCSW 2013)** 1487
  Ari Juels *(Unaffiliated),* Bryan Parno *(Microsoft Research)*
- **CCS'13 Co-Located Workshop Summary for SPSM 2013** 1489
  Adrienne Porter Felt *(Google, USA),* N. Asokan *(Aalto University & University of Helsinki)*

- **Smart Energy Grid Security Workshop (SEGS'13)** 1491
  Klaus Kursawe, Benessa Defend *(ENCS)*
- **Eighth ACM Workshop on Digital Identity Management (DIM 2013): Identity at the Crossroads** 1493
  Thomas Groß *(Newcastle University),* Marit Hansen *(Unabhängiges Landeszentrum für Datenschutz)*

Tutorial Overviews

- **Constructive and Destructive Aspects of Embedded Security in the Internet of Things** 1495
  Christof Paar *(Ruhr-Universität Bochum)*
- **Trusted Execution Environments on Mobile Devices** 1497
  Jan-Erik Ekberg *(Trustonic),* Kari Kostiainen *(ETH Zurich),* N. Asokan *(University of Helsinki)*
- **Easily Instrumenting Android Applications for Security Purposes** 1499
  Eric Bodden *(Technische Universität Darmstadt & Fraunhofer SIT)*

Author Index 1503

ACM CCS 2013 – Organization

General Chair:	Ahmad-Reza Sadeghi *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
Program Chairs:	Virgil Gligor *(Carnegie Mellon University, USA)*
	Moti Yung *(Columbia University, USA)*
Workshop Co-Chairs:	Stefan Katzenbeisser *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
	Christopher Kruegel *(University of California at Santa Barbara, USA)*
Tutorial Co-Chairs:	Thorsten Holz *(Ruhr-Universität Bochum, Germany)*
	Gregory Neven *(IBM Research, Zurich Research Laboratory, Switzerland)*
Poster/Demo Chairs:	Fabian Monrose *(University of North Carolina at Chapel Hill, USA)*
	Thomas Schneider *(TU Darmstadt, EC SPRIDE, Germany)*
	Carmela Troncoso *(Gradiant, Spain)*
Publicity Co-Chairs:	Thomas Gross *(University of Newcastle upon Tyne, UK)*
	Matthias Hollick *(TU Darmstadt, Germany)*
	Jun Li *(University of Oregon, USA)*
	Ivan Martinovic *(University of Oxford, UK)*
	Matthew Smith *(Leibnitz Universität Hannover, Germany)*
Event Management:	Wiebke Kronz *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
	Anette Mittenhuber *(TU Darmstadt, CASED, Germany)*
Public Relations:	Oliver Küch *(Fraunhofer SIT, CASED, Germany)*
Website:	Lucas Davi *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
Local Organization:	Stephan Heuser *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
	Christian Wachsmann, *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
	Christoph Busold *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
	Alexandra Dmitrienko *(Fraunhofer SIT, Germany)*
	Sven Wohlgemuth *(TU Darmstadt, CASED, Germany)*
	Mihai Bucicoiu *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
Steering Committee:	Elisa Bertino *(Purdue University, USA)*
	George Danezis *(Microsoft Research Cambridge, UK)*
	Trent Jaeger *(Pennsylvania State University, USA)*
	Carl Landwehr *(University of Maryland, USA)*
	John Mitchell *(Stanford University, USA)*
	Giovanni Vigna *(University of California at Santa Barbara, USA)*
	Marianne Winslet *(University of California at Urbana Champaign, USA)*

Program Committee: Gail-Joon Ahn *(Institute of North Carolina at Charlotte, USA)*
Bill Arbaugh *(University of Maryland, USA)*
Mikhail Atallah *(Purdue University, USA)*
Giuseppe Ateniese *(University of Rome, Italy)*
David Basin *(ETH Zurich, Swizerland)*
Lujo Bauer *(Carnegie Mellon University, USA)*
Konstantin Beznosov *(University of British Columbia, Canada)*
Matt Bishop *(University of California at Davis, USA)*
David Brumley *(Carnegie Mellon University, USA)*
Kevin Butler *(University of Oregon, USA)*
Jan Camenisch *(IBM Research, Zurich Research Laboratory, Swizerland)*
Srdjan Capkun *(ETH Zurich, Swizerland)*
Alvaro Cardenas *(University of Texas at Dallas, USA)*
Liqun Chen *(Hewlett-Packard Laboratories, UK)*
Stephen Chong *(Harvard University, USA)*
Nicolas Christin *(Carnegie Mellon University, USA)*
Veronique Cortier *(CNRS, Loria, France)*
Weidong Cui *(Microsoft Research, USA)*
Reza Curtmola *(New Jersey Institute of Technology, USA)*
Anupam Datta *(Carnegie Mellon University, USA)*
Roberto Di Pietro *(Università di Roma Tre, Italy)*
Wenliang Du *(Syracuse University,USA)*
David Evans *(University of Virginia, USA)*
Peter Gutmann *(University of Auckland, New Zealand)*
J. Alex Halderman *(University of Michigan, USA)*
Cormac Herley *(Microsoft Research, USA)*
Thorsten Holz *(Ruhr-Universität Bochum, Germany)*
Nicholas Hopper *(University of Minnesota, USA)*
Yih-Chun Hu *(University of Illinois at Urbana Champaign, USA)*
Sotiris Ioannidis *(FORTH-ICS, Greece)*
Trent Jaeger *(Pennsylvania State University, USA)*
Sushil Jajodia *(George Mason University, USA)*
Rob Johnson *(Stony Brook University, USA)*
Ari Juels *(RSA Laboratories, USA)*
Apu Kapadia *(Indiana University, USA)*
Jonathan Katz *(University of Maryland, USA)*
Stefan Katzenbeisser *(TU Darmstadt, CASED, Intel ICRI-SC, Germany)*
Angelos Keromytis *(Columbia University, USA)*
Florian Kerschbaum *(SAP Research, Germany)*
Yongdae Kim *(KAIST, Korea)*
Engin Kirda *(Northeastern University, USA)*
Farinaz Koushanfar *(Rice University, USA)*
Wenke Lee *(Georgia Institute of Technology, USA)*
Brian N. Levine *(UMass Amherst, USA)*
Yingjiu Li *(Singapore Management University, Singapore)*

Program Committee (continued):	Z. Morley Mao *(Columbia University, USA)*
	Jonathan McCune *(Google, USA)*
	Catherine Meadows *(Naval Research Laboratory, USA)*
	Refik Molva *(EURECOM, France)*
	Fabian Monrose *(University of North Carolina at Chapel Hill, USA)*
	Andrew Myers *(Cornell University, USA)*
	David Naccache *(Ecole Normale Supérieure, France)*
	Cristina Nita-Rotaru *(Purdue University, USA)*
	Alina Oprea *(RSA Security, USA)*
	Panos Papadimitratos (*KTH Stockholm, Sweden)*
	Bryan Parno *(Microsoft Research, USA)*
	Benny Pinkas *(Bar-Ilan University, Israel)*
	Mike Reiter *(University of North Carolina at Chapel Hill, USA)*
	Volker Roth *(Freie Universität Berlin, Germany)*
	Ravi Sandhu *(University of Texas at San Antonio, USA)*
	Vyas Sekar *(Stony Brook University, USA)*
	Simha Sethumadhavan *(Columbia University, USA*)
	Shiuhpyng Shieh *(National Chiao Tung University, Taiwan)*
	Clay Shields *(Georgetown University, USA)*
	Radu Sion *(Stony Brook University, USA)*
	Sean Smith *(Dartmouth College, USA)*
	Sal Stolfo *(Columbia University, USA)*
	Patrick Tague *(Carnegie Mellon University, USA)*
	Roberto Tamassia *(Brown University, USA)*
	George Theodorakopoulos *(Cardiff University, UK)*
	Wade Trappe *(Rutgers University, USA)*
	Patrick Traynor *(Georgia Institute of Technology, USA*)
	Carmela Troncoso *(Gradiant, Spain)*
	Vijay Varadharajan *(Macquarie University, Australia)*
	Michael Waidner *(Fraunhofer SIT, Germany)*
	Jesse Walker *(Intel, USA)*
	Bogdan Warinschi *(University of Bristol, UK)*
	Brent Waters *(University of Texas at Austin, USA)*
	Robert Watson *(Cambridge University, UK)*
	Nicholas Weaver *(ICSI, USA)*
	Dongyan Xu *(Purdue University, USA)*
Poster/Demo Program Committee:	Juan Caballero *(IMDEA Madrid, Spain)*
	Emiliano De Cristofaro *(PARC, USA)*
	William Enck *(North Carolina State University, USA)*
	Damon McCoy *(George Mason University, USA)*
	Prateek Mittal *(University of California at Berkeley, USA)*
	Thomas Ristenpart *(University of Wisconsin, USA)*
	Julie Thorpe *(University of Ontario Institute of Technology, Canada)*
	Ingrid Verbauwhede *(KU Leuven, Belgium)*

Additional Reviewers:

Amit Ahlawat
Massimiliano Albanese
Mohammed Almeshekah
Chaitrali Amrutkar
Elli Androulaki
Spyros Antonatos
Owen Arden
George Argyros
Aslan Askarov
Elias Athanasopoulos
Man Ho Au
Thanassis Avgerinos
Adam Aviv
Monir Azraoui
Basim Baig
Sumeet Bajaj
Ero Balsa
Davide Balzarotti
Boaz Barak
Adam Bates
Andrew Baumann
Alessandra De Benedictis
Emery Berger
David Bernhard
Sebastian Biedermann
Marina Blanton
Jeremiah Blocki
Nathaniel Boggs
Joseph Bonneau
Yazan Boshmaf
Kevin Bowers
Dan Brown
Christina Brzuska
Xiang Cai
Henry Carter
Sang Kil Cha
Rohit Chadha
Sambuddho Chakravarty
Sang-Yoon Chang
Peter Chapman
Chong-Kuan Chen
Pokai Chen
Vincent Cheval

Jerry Chiang
Michael Cheng Yi Cho
Hyunwoo Choi
Jaeyoung Choi
Kai-Min Chung
Michael Clarkson
Robert Cochran
Alessandro Colantonio
Cas Cremers
Emiliano De Cristofaro
Özgür Dagdelen
George Danezis
Mohammad Torabi Dashti
Lucas Davi
Zhui Deng
Alexandra Dmitrienko
Yevgeniy Dodis
Adam Doupe
Maria Dubovitskaya
Manuel Egele
Kaoutar Elkhiyaoui
William Enck
Robert Enderlein
Santiago Escobar
Antonio Faonio
Dario Fiore
Aurélien Francillon
Mario Frank
Sara Foresti
David Galindo
Deepak Garg
Paolo Gasti
Robert Gawlik
Xinyang Ge
John Geddes
Marco Ghiglieri
Ian Goldberg
Samantha Gottlieb
Robert Griffin
Oren Halvani
Kevin Hamlen
Kristiyan Haralambiev
Eiji Hayashi

Carmit Hazay
Nadia Heninger
Ryan Henry
Victor Heorhiadi
Michael Herrmann
Martin Hirt
Johannes Hoffmann
Owen Hofmann
Peter Honeyman
Byeongdo Hong
Hyunwook Hong
Endadul Hoque
Chia-Wei Hsu
Hongxin Hu
Yan Huang
Markus Huber
Sungjae Hwang
Qatrunnada Ismail
Malika Izabachene
Asim Jamshed
Kangkook Jee
Limin Jia
Xing Jin
Yiming Jing
Andrew Johnson
Lukas Kalabis
Seny Kamara
Nikos Karapanos
Nikolaos Karvelas
Michael Kasper
James Kelley
Vasileios P Kemerlis
Peter Kieseberg
Dongkwan Kim
Eunsoo Kim
Hongil Kim
Yu Seung Kim
Markulf Kohlweiss
Saranga Komanduri
Joonho Kong
Divyan Konidala
Georgios Kontaxis
Kari Kostiainen

Steve Kremer
Stephan Krenn
Christopher Kruegel
Marc Kuehrer
Anil KurmusChinawat Isradisaikul
Divya Kurthakoti
Cheolhyun Kwak
Minhee Kwon
Alptekin Küpçü
Tanja Lange
Adam Langley
Meixing Le
Hyojeong Lee
Youjin Lee
Anja Lehmann
Iraklis Leontiadis
Chaz Lever
Bing-Han Li
Ninghui Li
Peng Li
Shuai Li
Alana Libonati
Jed Liu
Giovanni Livraga
Andreas Lochbihler
Flavio Lombardi
Long Lu
Giuseppe Antonio Di Luna
Tongbo Luo
Tom Magrino
Ahmad Mahmoody
Ken Mai
Claudio Marforio
Matthew Maurer
Michelle Mazurek
Breno De Medeiros
Carlos Medrano
Byungho Min
Kazuhiro Minami
Bruno Conchina Montalto
Benjamin Mood
Scott Moore
Collin Mulliner
Arslan Munir
Divya Muthukumaran

Ryan Riley
Thomas Ristenpart
Shishir Nagaraja
Gregory Neven
Andrew Newell
Rishab Nithyanand
Adam O'Neill
Olga Ohrimenko
Melek Önen
Simon Oya
Omkant Pandey
Antonis Papadogiannakis
Charalampos Papamanthou
Vasilis Pappas
Ravi Pappu
Chunsung Park
Kenneth Paterson
Kenny Paterson
Sameer Patil
Arpita Patra
Mathias Payer
Marcus Peinado
Andreas Peter
Theofilos Petsios
Patrick Longa Pierola
Jérémy Planul
Joe Pletcher
Iasonas Polakis
Michalis Polychronakis
Marios Pomonis
Miodrag Potkonjak
Franz-Stefan Preiss
Pasquale Puzio
Sasa Radomirovic
Carla Rafols
Himanshu Raj
Kim Ramchen
Paul Ratazzi
Sasa Rdomirovic
Joel Reardon
Brad Reaves
Alexandre Rebert
Tazchy Reinman
Junghwan Rhee
Alfredo Rial

Ben Riva
Jean-Marc Robert
Masoud Rostami
Yves Roudier
Yannis Rouselakis
Arnab Roy
Carlos Rubio
Sandra Rueda
Malek Ben Salem
Brendan Saltaformaggio
Ralf Sasse
Guillaume Scerri
Thomas Schneider
Sebastian Schrittwieser
Max Schuchard
Steffen Schulz
Matthias Schunter
Edward Schwartz
Elaine Shi
Dongwan Shin
Hocheol Shin
Reza Shokri
Matteo Signorini
Hervais Simo
Dimitrios Simos
Arunesh Sinha
Karsten Sohr
Yingbo Song
Ebrahim Songhori
Claudio Soriente
Kyle Soska
Angelo Spognardi
Christoph Sprenger
Dannie Stanley
Emil Stefanov
Martin Stopczynski
William Sumner
Kun Sun
Yuqiong Sun
Gelareh Taban
Nirupama Talele
Rob Templeman
Stefano Tessaro
Abhradeep Guha Thakurta
Nikos Triandopoulos

Mahesh Tripunitara
Jonathan Trostle
Michael Carl Tschantz
Uday Tupakula
Mathieu Turuani
Yavgeniy Vahlis
Giorgos Vasiliadis
Amit Vasudevan
Daniele Venturi
Nino Vincenzo Verde
Giovanni Vigna
Hayawardh Vijayakumar
Antonio Villani
Sabrina De Capitani Di Vimercati
Jonathan Voris
Adam Waksman

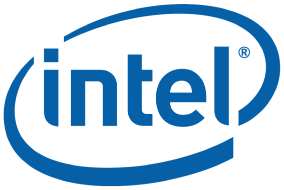
Robert Walls
Chi-Wei Wang
Chiawei Wang
Lingyu Wang
Shumiao Wang
Yang Wang
Zhan Wang
Gaven J Watson
Lei Wei
Zachary Weinberg
Cyrille Wiedling
Peter Williams
Maverick Woo
Eric Wustrow
Qiang Yan
Dejun Yang

York Yannikos
Ting-Fang Yen
Yung Yi
Jun Yuan
Angeliki Zavou
Danfeng Zhang
Yinqian Zhang
Yizhou Zhang
Zhi-Kai Zhang
Hang Zhao
Ziming Zhao
Lan Zhou
Zhibin Zhou
Sebastian Zimmeck

CCS 2013 Sponsor & Supporters

Sponsor:

Supporters:



Supporters (continued):

heise Security

Microsoft Research

NXP

KOBIL secure your identity

Sirrix AG security technologies

certgate

IBM Research