

Alexandria, Virginia, USA
October 29–November 2, 2007



Association for
Computing Machinery

Advancing Computing as a Science & Profession



CCS'07

Proceedings of the 14th ACM Conference on
Computer and Communications Security

Sponsored by:

ACM SIGSAC

and supported by:

**Army Research Office, Cisco Research Center, Google,
IBM Research, and Microsoft Research**

Edited by:

Sabrina De Capitani di Vimercati, Paul Syverson, & David Evans



**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 © 2007 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: Publications Dept., ACM, Inc. Fax +1 (212) 869-0481 or <permissions@acm.org>.

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 the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

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: 978-1-59593-703-2

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 11405
New York, NY 10286-1405

Phone: 1-800-342-6626
(US and Canada)
+1-212-626-0500
(all other countries)
Fax: +1-212-944-1318
E-mail: acmhelp@acm.org

ACM Order Number 537070

Printed in the USA

Welcome to CCS 2007

It is a pleasure and honor to welcome you to the 14th ACM Conference on Computer and Communications Security. This year's conference continues and extends its tradition as a premier forum for new data-security research. We have an excellent program comprising two research tracks, an industry track, three tutorials, and ten workshops. The conference covers a strikingly broad spectrum of interests and disciplines in the area of computer and communications security.

The conference has benefited from many contributors to its success. I would like to thank Sabrina De Capitani di Vimercati and Paul Syverson, the research-track program co-chairs, along with the members of their program committee. The research program remains very highly selective, as evidenced by the caliber of the papers even more than acceptance statistics. My thanks also to the industry-track chair, Patrick McDaniel, and his program committee for arranging talks on applied topics to complement the other conference offerings.

I would like to extend my appreciation to Vijay Atluri, the workshops chair, for assembling a broad, strong program of workshops and ensuring their smooth execution. I would also like to thank all the workshop program-chairs, specifically: Ravi Sandhu and Jon A. Solworth (Workshop on Computer Security Architecture); Gail-Joon Ahn, Elisa Bertino, Jan Camenisch, and Howard Lipson (Workshop on Digital Identity Management); Aggelos Kiayias and Ahmad Reza-Sadeghi (Workshop on Digital Rights Management); Virgil Gligor and Heiko Mantel (Workshop on Formal Methods in Security Engineering: From Specifications to Code); Ting Yu (Workshop on Privacy in Electronic Society); Günter Karjoth and Ketil Stølen (Workshop on Quality of Protection); Christopher Kruegel (Workshop on Recurring Malcode); Valerie Henson (Workshop on Storage Security and Survivability); Shouhuai Xu and Moti Yung (Workshop on Scalable Trusted Computing); and Ernesto Damiani and Seth Proctor (Workshop on Secure Web Services). I would also like to express my thanks to Wenliang (Kevin) Du for a strong program of tutorials.

I am grateful to Steve Lipner for delivering the keynote address. My thanks as well to those who have offered their untiring administrative support, namely to Sencun Zhu for managing the budget, David Evans for assisting with the preparation of the proceedings, and Radha Poovendran and his assistant Krishna Sampigethaya for the publicity of the conference. I wish to express my appreciation to the CCS steering committee, Sushil Jajodia (Chair), Carl Gunter, Ravi Sandhu, and Pierangela Samarati, for their help with myriad logistical questions. I would also like to acknowledge the administrative staff of the ACM SIGSAC and George Mason University for their support, and Executive Events for its management of the registration process. In particular, I would not have survived as the general chair without the excellent work of Karen Tai at George Mason University, who handled almost all of the logistical tasks. Finally, I wish to thank the following institutions for their generous financial contribution: The Army Research Office, Cisco Research Center, Google, IBM Research, and Microsoft Research.

I hope that you, the conference and workshop attendees, will find this year's programs stimulating and beneficial for your research. Welcome—and enjoy.

Peng Ning
General Chair
ACM CCS 2007

Message from the Program Chairs

These proceedings contain the papers selected for presentation at the *14th ACM Conference on Computer and Communications Security (CCS 2007)*, held October 29 to November 2, 2007 in Alexandria, VA, USA.

In response to the call for papers 302 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the program committee. Reviewing was double-blind, meaning that the program committee was not able to see the names and affiliations of the authors, and the authors were not told which committee members reviewed which papers. After the reviews were written, the program committee met online for three weeks of intensive discussion. Of the papers submitted, 55 were selected for presentation at the conference, giving an acceptance rate of about 18%.

There is a long list of people who volunteered their time and energy to put together the conference and who deserve acknowledgment. Thanks to all the members of the program committee, and the external reviewers, for all their hard work in evaluating and discussing papers. We would like to thank the members of the steering committee, Sushil Jajodia, Carl A. Gunter, Pierangela Samarati, and Ravi Sandhu, for their support. We are also very grateful to all other CCS 2007 organizers whose work ensured a smooth organizational process.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you find the program stimulating.

Sabrina De Capitani di Vimercati

CCS 2007 Research Track

Program Chair

Paul Syverson

CCS 2007 Research Track

Program Chair

Table of Contents

CCS 2007 Organization	xi
------------------------------------	----

Keynote

Session Chair: Sabrina De Capitani di Vimercati (*University of Milan*)

- **Assurance and Evaluation: What Next?** 1
Steven B. Lipner (*Microsoft Corporation*)

Session 1: Web Applications Security

Session Chair: Marianne Winslett (*University of Illinois*)

- **An Analysis of Browser Domain-Isolation Bugs and a Light-Weight Transparent Defense Mechanism**..... 2
Shuo Chen (*Microsoft Research*), David Ross (*Microsoft*), Yi-Min Wang (*Microsoft Research*)
- **CANDID: Preventing SQL Injection Attacks Using Dynamic Candidate Evaluations**..... 12
Sruthi Bandhakavi (*University of Illinois, Urbana Champaign*),
Prithvi Bisht (*University of Illinois, Chicago*),
P. Madhusudan (*University of Illinois, Urbana-Champaign*),
V. N. Venkatakrishnan (*University of Illinois, Chicago*)
- **Multi-Module Vulnerability Analysis of Web-based Applications**..... 25
Davide Balzarotti, Marco Cova, Viktoria V. Felmetzger, Giovanni Vigna
(*University of California, Santa Barbara*)

Session 2: Authentication and Passwords

Session Chair: Jianying Zhou (*Institute for Infocomm Research*)

- **Do Background Images Improve “Draw a Secret” Graphical Passwords?** 36
Paul Dunphy, Jeff Yan (*Newcastle University*)
- **BeamAuth: Two-Factor Web Authentication with a Bookmark**..... 48
Ben Adida (*Harvard University*)
- **Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers** 58
Chris Karlof, J. D. Tygar, David Wagner (*University of California, Berkeley*),
Umesh Shankar (*Google, Inc.*)

Session 3: Anonymity

Session Chair: Claudia Diaz (*K.U. Leuven*)

- **Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs** 72
Patrick P. Tsang (*Dartmouth College*), Man Ho Au (*University of Wollongong*),
Apu Kapadia, Sean W. Smith (*Dartmouth College*)
- **How Much Anonymity Does Network Latency Leak?** 82
Nicholas Hopper, Eugene Y. Vasserman, Eric Chan-Tin (*University of Minnesota*)
- **Denial of Service or Denial of Security?** 92
Nikita Borisov (*University of Illinois at Urbana-Champaign*), George Danezis (*K.U. Leuven*),
Prateek Mittal (*University of Illinois at Urbana-Champaign*), Parisa Tabriz (*Google*)

Session 4: Operating Systems and Malware

Session Chair: Sencun Zhu (*The Pennsylvania State University*)

- **Automated Detection of Persistent Kernel Control-Flow Attacks** 103
Nick L. Petroni, Jr., Michael Hicks (*University of Maryland, College Park*)

- **Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis** 116
Heng Yin (*Carnegie Mellon University & College of William and Mary*),
Dawn Song (*University of California at Berkeley & Carnegie Mellon University*),
Manuel Egele, Christopher Kruegel, Engin Kirda (*Technical University Vienna*)
- **Stealthy Malware Detection Through VMM-Based Out-of-the-Box” Semantic View Reconstruction”** 128
Xuxian Jiang, Xinyuan Wang (*George Mason University*), Dongyan Xu (*Purdue University*)

Session 5: Traffic Analysis and Location Privacy

Session Chair: Peng Liu (*The Pennsylvania State University*)

- **Shunting: A Hardware/Software Architecture for Flexible, High-Performance Network Intrusion Prevention** 139
Jose M. Gonzalez, Vern Paxson, Nicholas Weaver (*International Computer Science Institute*)
- **Highly Efficient Techniques for Network Forensics** 150
Miroslav Pone, Paul Giura, Hervé Brönnimann, Joel Wein (*Polytechnic University*)
- **Preserving Privacy in GPS Traces via Uncertainty-Aware Path Cloaking** 161
Baik Hoh, Marco Gruteser, Hui Xiong (*Rutgers University*),
Ansa Alrabady (*General Motors Corporation*)

Session 6: Cryptography

Session Chair: Gene Tsudik (*University of California, Irvine*)

- **Robust Computational Secret Sharing and a Unified Account of Classical Secret-Sharing Goals** 172
Mihir Bellare (*University of California, San Diego*), Phillip Rogaway (*University of California, Davis*)
- **Chosen-Ciphertext Secure Proxy Re-Encryption** 185
Ran Canetti (*IBM T.J. Watson Research Center*),
Susan Hohenberger (*The Johns Hopkins University*)
- **Attribute-Based Encryption with Non-Monotonic Access Structures** 195
Rafail Ostrovsky, Amit Sahai (*University of California, Los Angeles*), Brent Waters (*SRI International*)

Session 7: Network Security

Session Chair: Rachel Greenstadt (*Harvard University*)

- **Optimal Security Hardening Using Multi-objective Optimization on Attack Tree Models of Networks** 204
Rinku Dewri, Nayot Poolsappasit, Indrajit Ray, Darrell Whitley (*Colorado State University*)
- **On the Accuracy of Decentralized Virtual Coordinate Systems in Adversarial Networks** 214
David John Zage, Cristina Nita-Rotaru (*Purdue University*)
- **Analyzing the Vulnerability of Superpeer Networks Against Attack** 225
B. Mitra (*Indian Institute of Technology, Kharagpur*), F. Peruani (*Technical University of Dresden*),
S. Ghose, N. Ganguly (*Indian Institute of Technology, Kharagpur*)
- **Towards Automated Provisioning of Secure Virtualized Networks** 235
Serdar Cabuk, Chris I. Dalton (*Hewlett-Packard Laboratories*),
HariGovind Ramasamy, Matthias Schunter (*IBM Zurich Research Laboratory*)

Session 8: Election Systems and Applied Cryptography

Session Chair: Matt Edman (*Rensselaer Polytechnic Institute*)

- **Split-Ballot Voting: Everlasting Privacy With Distributed Trust** 246
Tal Moran, Moni Naor (*Weizmann Institute of Science*)
- **An Independent Audit Framework for Software Dependent Voting Systems** 256
Sujata Garera, Aviel D. Rubin (*Johns Hopkins University*)

- **Forward-Secure Signatures in Untrusted Update Environments: Efficient and Generic Constructions**266
Benoi Libert (*Université Catholique de Louvain*),
Jean-Jacques Quisquater (*Université Catholique de Louvain*),
Moti Yung (*Columbia University*)
- **Ordered Multisignatures and Identity-Based Sequential Aggregate Signatures, with Applications to Secure Routing**276
Alexandra Boldyreva (*Georgia Institute of Technology*), Craig Gentry (*Stanford University*),
Adam O'Neill (*Georgia Institute of Technology*), Dae Hyun Yum (*POSTECH*)

Session 9: Side and Covert Channels Detection

Session Chair: Matthew Wright (*University of Texas at Arlington*)

- **An Information-Theoretic Model for Adaptive Side-Channel Attacks**286
Boris Köpf, David Basin (*ETH Zurich*)
- **Covert Channels in Privacy-Preserving Identification Systems**297
Daniel V. Bailey (*RSA Laboratories*), Dan Boneh, Eu-Jin Goh (*Stanford University*),
Ari Juels (*RSA Laboratories*)
- **Detecting Covert Timing Channels: An Entropy-Based Approach**307
Steven Gianvecchio, Haining Wang (*The College of William and Mary*)

Session 10: Protocols and Spam Filters

Session Chair: Sven Dietrich (*Stevens Institute of Technology*)

- **Polyglot: Automatic Extraction of Protocol Message Format using Dynamic Binary Analysis**317
Juan Caballero (*Carnegie Mellon University*),
Heng Yin (*College of William and Mary & Carnegie Mellon University*),
Zhenkai Liang (*Carnegie Mellon University*),
Dawn Song (*University of California, Berkeley & Carnegie Mellon University*)
- **Harvesting Verifiable Challenges from Oblivious Online Sources**330
J. Halderman (*Princeton University*), Brent Waters (*SRI International*)
- **Filtering Spam with Behavioral Blacklisting**342
Anirudh Ramachandran, Nick Feamster, Santosh Vempala (*Georgia Institute of Technology*)

Session 11: Internet Security

Session Chair: Roger Dingledine (*The Tor Project*)

- **ConceptDoppler: A Weather Tracker for Internet Censorship**352
Jedidiah R. Crandall (*University of New Mexico*),
Daniel Zinn, Michael Byrd, Earl Barr (*University of California, Davis*),
Rich East (*Independent Researcher*)
- **Asirra: A CAPTCHA That Exploits Interest-Aligned Manual Image Categorization**366
Jeremy Elson, John R. Douceur, Jon Howell (*Microsoft Research*),
Jared Saul (*Petfinder, Inc.*)
- **An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants**375
Jason Franklin (*Carnegie Mellon University*), Vern Paxson (*ICSI*),
Adrian Perrig (*Cylab & Carnegie Mellon University*), Stefan Savage (*University of California, San Diego*)

Session 12: Key Management

Session Chair: Radu Sion (*Stony Brook University*),

- **Hardware-rooted Trust for Secure Key Management and Transient Trust**389
Jeffrey S. Dworkin, Ruby B. Lee (*Princeton University*)

- **Robust Key Generation from Signal Envelopes in Wireless Networks** 401
Babak Azimi-Sadjadi (*Intelligent Automation, Inc.*), Aggelos Kiayias (*University of Connecticut*),
Alejandra Mercado (*Rensselaer Polytechnic Institute and Hughes Network Systems*),
Bulent Yener (*Rensselaer Polytechnic Institute*)
- **Robust Group Key Agreement Using Short Broadcasts** 411
Stanisław Jarecki, Jihye Kim, Gene Tsudik (*University of California, Irvine*)

Session 13: Policies

Session Chair: William Winsborough (*University of Texas at San Antonio*)

- **Protecting Browsers from DNS Rebinding Attacks** 421
Collin Jackso, Adam Barth, Andrew Bortz, Weidong Shao, Dan Boneh (*Stanford University*)
- **Alpaca: Extensible Authorization for Distributed Services** 432
Chris Lesniewski-Laas, Bryan Ford, Jacob Strauss, Robert Morris, M. Frans Kaashoek
(*Massachusetts Institute of Technology*)
- **Efficient Policy Analysis for Administrative Role Based Access Control** 445
Scott D. Stoller (*Stony Brook University*), Ping Yang (*Binghamton University*),
C. R. Ramakrishnan (*Stony Brook University*), Mikhail I. Gofman (*Binghamton University*)

Session 14: Cryptography and Cryptoanalysis

Session Chair: Ari Juels (*RSA Laboratories*)

- **Provably Secure Ciphertext Policy ABE** 456
Ling Cheung, Calvin Newport (*Massachusetts Institute of Technology*)
- **Security Under Key-Dependent Inputs** 466
Shai Halevi, Hugo Krawczyk (*IBM T.J. Watson Research Center*)
- **Cryptanalysis of the Windows Random Number Generator** 476
Leo Dorrendorf, Zvi Gutterman (*The Hebrew University of Jerusalem*), Benny Pinkas (*University of Haifa*)

Session 15: Data Privacy

Session Chair: Wenliang (Kevin) Du (*Syracuse University*)

- **Secure Two-Party k-Means Clustering** 486
Paul Bunn, Rafail Ostrovsky (*University of California, Los Angeles*)
- **Privacy-Preserving Remote Diagnostics** 498
Justin Brickell, Donald E. Porter, Vitaly Shmatikov, Emmett Witchel (*The University of Texas at Austin*)
- **Automaton Segmentation: A New Approach to Preserve Privacy in XML Information Brokering** 508
Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, Chao-Hsien Chu (*The Pennsylvania State University*)
- **Privacy Preserving Error Resilient DNA Searching through Oblivious Automata** 519
Juan Ramón Troncoso-Pastoriza (*University of Vigo*), Stefan Katzenbeisser (*Philips Research Europe*),
Mehmet Celik (*Philips Research Europe*)

Session 16: Software Security

Session Chair: Nick Weaver (*International Computer Science Institute*)

- **Predicting Vulnerable Software Components** 529
Stephan Neuhaus (*Saarland University*), Thomas Zimmermann (*University of Calgary*),
Christian Holler, Andreas Zeller (*Saarland University*)
- **On the Infeasibility of Modeling Polymorphic Shellcode** 541
Yingbo Song, Michael E. Locasto, Angelos Stavrou, Angelos D. Keromytis, Salvatore J. Stolfo
(*Columbia University*)

- **The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86)** 552
Hovav Shacham (*University of California, San Diego*)
- **MemSherlock: An Automated Debugger for Unknown Memory Corruption Vulnerabilities** 562
Emre C. Sezer, Peng Ning, Chongkyung Kil (*North Carolina State University*), Jun Xu (*Google, Inc.*)

Session 17: Data Disclosure

Session Chair: Vitaly Shmatikov (*University of Texas at Austin*)

- **Information Disclosure under Realistic Assumptions: Privacy versus Optimality** 573
Lei Zhang, Sushil Jajodia, Alexander Brodsky (*George Mason University*)
- **PORs: Proofs of Retrievability for Large Files** 584
Ari Juels (*RSA Laboratories*), Burton S. Kaliski Jr. (*EMC Corporation*)
- **Provable Data Possession at Untrusted Stores** 598
Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring (*Johns Hopkins University*),
Lea Kissner (*Google, Inc.*), Zachary Peterson (*Johns Hopkins University*),
Dawn Song (*University of California, Berkeley & Carnegie Mellon University*)

Author Index 611

CCS 2007 Conference Organization

General Chair: Peng Ning (*NC State University, USA*)

Program Co-Chairs: Sabrina De Capitani di Vimercati (*University of Milan, Italy*)
Paul Syverson (*Naval Research Laboratory, USA*)

Industry & Government Track Chair: Patrick McDaniel (*Penn State University, USA*)

Publicity Chair: Radha Poovendran (*University of Washington, USA*)

Publication Chair: David Evans (*University of Virginia, USA*)

Tutorials Chair: Wenliang (Kevin) Du (*Syracuse University, USA*)

Treasurer: Sencun Zhu (*Penn State University, USA*)

Workshops Chair: Vijay Atluri (*Rutgers University, USA*)

Steering Committee: Sushil Jajodia (*George Mason University, USA*)
Carl A. Gunter (*University of Illinois, USA*)
Pierangela Samarati (*University of Milan, Italy*)
Ravi Sandhu (*University of Texas, San Antonio, USA*)

Program Committee: Martín Abadi (*UC Santa Cruz & Microsoft Research, USA*)
Gail-Joon Ahn (*UNC Charlotte, USA*)
Mikhail Atallah (*Purdue University, USA*)
Giuseppe Ateniese (*The Johns Hopkins University, USA*)
Vijay Atluri (*Rutgers University, USA*)
Dan Boneh (*Stanford University, USA*)
Lorrie Cranor (*Carnegie Mellon University, USA*)
Marco Cremonini (*University of Milan, Italy*)
David Dagon (*Georgia Institute of Technology, USA*)
George Danezis (*K.U. Leuven, Belgium*)
Robert Deng (*Singapore Management University, Singapore*)
Claudia Diaz (*K.U. Leuven, Belgium*)
Sven Dietrich (*Carnegie Mellon University, USA*)
Roger Dingledine (*The Free Haven Project, USA*)
Wenliang (Kevin) Du (*Syracuse University, USA*)
Matt Edman (*Rensselaer Polytechnic Institute, USA*)
Alberto Escudero-Pascual (*IT46, Sweden*)
Simone Fischer-Huebner (*Karlstad University, Sweden*)
Virgil Gligor (*University of Maryland at College Park, USA*)
Philippe Golle (*Palo Alto Research Center, USA*)
Dieter Gollmann (*TU Hamburg-Harburg, Germany*)
Rachel Greenstadt (*Harvard University, USA*)
Markus Jakobsson (*Indiana University, USA*)

Program Committee

(continued): Somesh Jha (*University of Wisconsin, USA*)
Ari Juels (*RSA Laboratories, USA*)
Angelos Keromytis (*Columbia University, USA*)
Christopher Kruegel (*Technical University Vienna, Austria*)
Xuejia Lai (*Shanghai Jiaotong University, China*)
Wenke Lee (*Georgia Institute of Technology, USA*)
Peng Liu (*The Pennsylvania State University, USA*)
Heiko Mantel (*RWTH Aachen, Germany*)
Nick Mathewson (*The Free Haven Project, USA*)
John McHugh (*Dalhousie University, Canada*)
Ludovic Mé (*Supélec, France*)
Catherine Meadows (*Naval Research Laboratory, USA*)
Gerome Miklau (*University of Massachusetts, USA*)
John Mitchell (*Stanford University, USA*)
David Molnar (*UC Berkeley, USA*)
Yi Mu (*University of Wollongong, Australia*)
Steven Murdoch (*University of Cambridge, UK*)
Stefano Paraboschi (*University of Bergamo, Italy*)
Bart Preneel (*K.U. Leuven, Belgium*)
Peter Ryan (*Newcastle University, UK*)
Kazue Sako (*NEC Corporation, Japan*)
Pierangela Samarati (*University of Milan, Italy*)
Shiuhpyng Shieh (*National Chiao Tung University, Taiwan*)
Vitaly Shmatikov (*University of Texas, USA*)
Radu Sion (*Stony Brook, USA*)
Einar Snekkenes (*Gjøvik University College, Norway*)
Salvatore Stolfo (*Columbia University, USA*)
Jonathan T. Trostle (*ASK Consulting and Research, USA*)
Nicholas Weaver (*Int. Computer Science Institute, USA*)
Vicky Weissman (*Cornell University, USA*)
William Winsborough (*Univ. of Texas at San Antonio, USA*)
Marianne Winslett (*University of Illinois, USA*)
Matthew Wright (*University of Texas at Arlington, USA*)
Alec Yasinsac (*Florida State University, USA*)
Ting Yu (*North Carolina State University, USA*)
Jianying Zhou (*Institute for Infocomm Research, Singapore*)
Sencun Zhu (*The Pennsylvania State University, USA*)
Mary Ellen Zurko (*IBM, USA*)

Additional reviewers:	Asmaa Adnane	Guofei Gu
	Periklis Akritidis	Qi Guo
	Kostas Anagnostakis	Yu-Lun Huang
	Christer Andersson	Wei Han
	Elena Andreeva	Ragib Hasan
	Manos Antonakakis	Hans Hedbom
	Toshinori Araki	Tom Heydt-Benjamin
	Christophe Bidan	Susan Hohenberger
	Joonsang Baek	Xuan Hong
	Farshad Bahari	Hongxin Hu
	Daniel V. Bailey	Shih-Kun Huang
	Sruthi Bandhakavi	Xinyi Huang
	Adam Barth	Shih-I Huang
	Lejla Batina	Yong Ho Hwang
	Marina Blanton	Sotiris Ioannidis
	Marcela Boboila	Keith Irwin
	Matt Burnside	Toshiyuki Isshiki
	Sebastien Canard	Collin Jackson
	Jan Cappaert	Karthick Jayaraman
	Martim Carbone	Yoon-Chan Jhi
	Bogdan Carbunar	Jing Jin
	Rong-Jaye Chen	Nenad Jovanovic
	Raymond Choo	Seny Kamara
	Mihai Christodorescu	Dong Seong Kim
	Richard Clayton	Engin Kirda
	Danny De Cock	Moonam Ko
	Robert Cole	Markulf Kohlweiss
	Debra Cook	Kameswari Kotapati
	Reza Curtmola	Louis Kruger
	Neil Daswani	Markus Kuhn
	Zijian Deng	Zhuowei Li
	Ling Dong	Soo Bum Lee
	Will Dormann	Adam J. Lee
	Filiol Eric	Francois Lesueur
	Úlfar Erlingsson	Fengjun Li
	Anna Lisa Ferrara	Dongyi Li
	Jun Furukawa	Lunquan Li
	Vinod Ganapathy	Zhuowei Li
	Rosario Gennaro	Alex X. Liu
	Craig Gentry	Michael Locasto
	Benedikt Gierlichs	Yu Long
	Zheng Gong	Haibing Lu
	Mike Gordon	Xianhui Lu
	Matthew Green	Di Ma

Additional reviewers**(continued):**

Xiaonan Ma	Henning Sudbrock
Leonardo Martucci	Xiaorui Sun
Jeffrey T. McDonald	Takehiro Takahashi
Nele Mentens	Isamu Teranishi
Kazuhiro Minami	Vrizlynn Thing
Soumyadeb Mitra	ValÈrie Viet Triem Tong
Kengo Mori	Eric Totel
Benjamin Morin	Carmela Troncoso
Steven Myers	Pim Tuyls
Arvind Narayanan	Frederik Vercauteren
Ching Y. Ng	Zhiguo Wan
Satoshi Obana	Xiaofeng Wang
Amon Ott	Xinran Wang
Bryan Payne	Hao Wang
Andy Parrish	Robert Watson
Napoleon Paxton	Sam Weiler
Gerardo Pelosi	Peter Williams
Slobodan Petrovic	Gilbert Wondracek
Murillo Pontual	Qianhong Wu
Alexander Reinhard	Yongdong Wu
Mohammad Reza Reyhanitabar	Chao Xia
Len Sassaman	Liang Xie
Dries Schellekens	Wenjuan Xu
Andrei Serjantov	Jeff Yan
Stefaan Seys	Ming-Hour Yang
Monirul Sharif	Yi Yang
Dongwan Shin	Yanjiang Yang
Ji Sun Shin	Wuu Yang
Heechang Shin	Yi-Shiung Yeh
Stelios Sidiroglou	Arkady Yerukhimovich
Randy Smith	Wanyu Zang
Chris Soghoian	Junjie Zhang
Yingbo Song	Qing Zhang
Rafael de Sousa	Charles Zhang
Sid Stamm	Jinmin Zhong
Angelos Stavrou	Minaxi Gupta
Liz Stinson	Xinran Wang

Sponsor:



Supporters:



Cisco Research Center

Google IBM Research

Microsoft®
Research