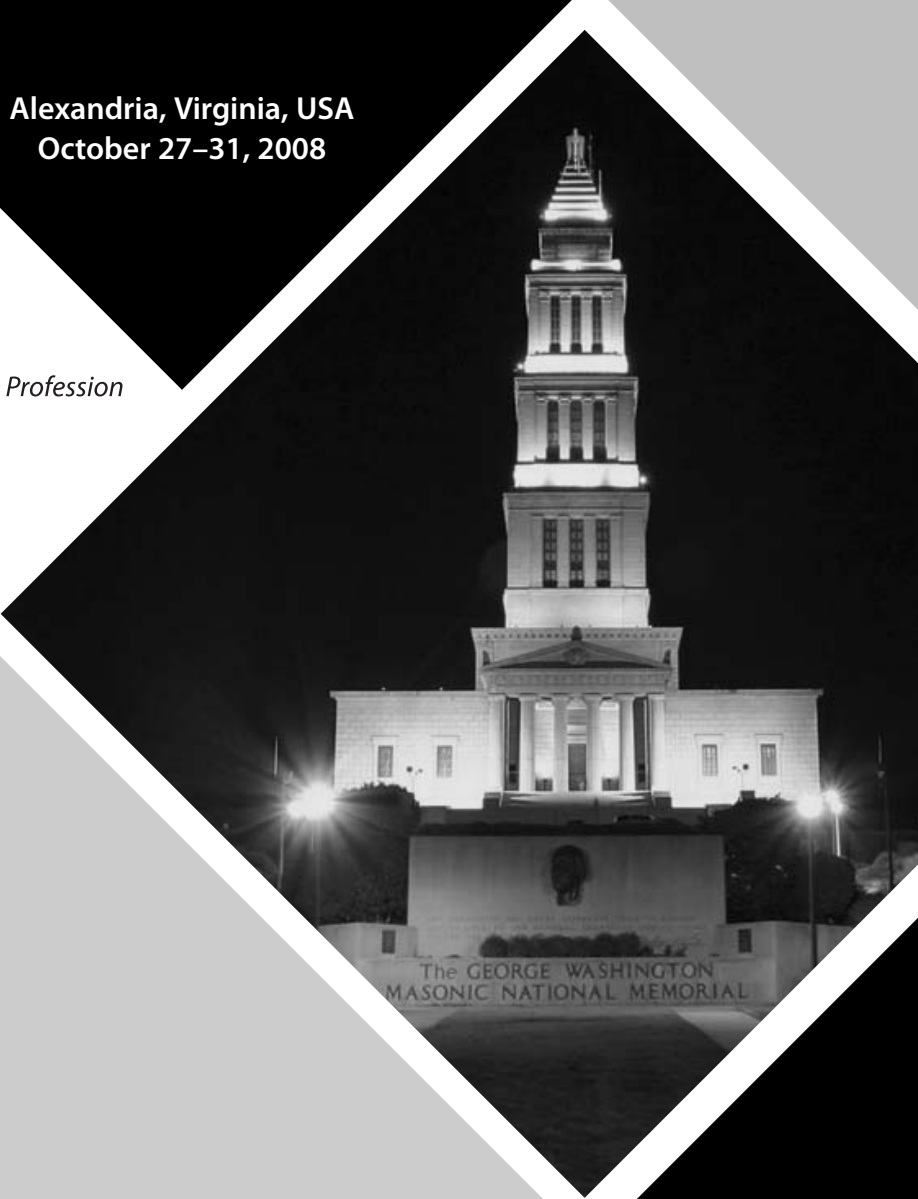


Alexandria, Virginia, USA
October 27–31, 2008



Association for
Computing Machinery

Advancing Computing as a Science & Profession



CCS'08

Proceedings of the 15th ACM Conference on
Computer and Communications Security

Sponsored by:

ACM SIGSAC

Supported by:

**Army Research Office, Dartmouth Institute for Security
Technology Studies, Google, IBM Research, Microsoft Research,
and Motorola**

Edited by:

Paul Syverson, Somesh Jha, & Xiaolan Zhang



**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 © 2008 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: 978-1-59593-810-7

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 537080

Printed in the USA

Welcome to CCS 2008

It is a pleasure and honor to welcome you to the 15th 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, twelve workshops, and a number of tutorials. 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 the program co-chairs, Paul Syverson and Somesh Jha, 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.

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: Dirk Balfanz and Jessica Staddon (Workshop on AISEC); Trent Jaeger (Workshop on Computer Security Architecture); Elisa Bertino and Kenji Takahashi (Workshop on Digital Identity Management); Gregory Heileman and Marc Joye (Workshop on Digital Rights Management); Vitaly Shmatikov (Workshop on Formal Methods in Security Engineering); Bill Yurcik (Workshop on Network Data Anonymization); Marianne Winslett (Workshop on Privacy in the Electronic Society); Andy Ozment and Ketil Stølen (Workshop on Quality of Protection); Yongdae Kim (Workshop on Storage Security and Survivability); Jean-Pierre Seifert and Cristina Nita-Rotaru (Workshop on Scalable Trusted Computing); Ernesto Damiani and Seth Proctor (Workshop on Secure Web Services); and Jason Nieh and Angelos Stavrou (Workshop on Virtual Machine Security). I would also like to express my thanks to Pierangela Samarati for a strong program of tutorials.

I am grateful to Martín Abadi 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, Ting Yu for maintaining the conference website and attending to my numerous requests, Xiaolan Zhang for assisting with the preparation of the proceedings, and Radha Poovendran for the publicity of the conference. I wish to express my appreciation to the rest of the CCS steering committee, Carl Gunter (Chair), Pierangela Samarati, Paul Syverson, Gene Tsudik, and Moti Young for their help. 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, Dartmouth Institute for Security Technology Studies, Google, IBM Research, Microsoft Research, and Motorola.

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 2008

Message from the Program Chairs

These proceedings contain the papers selected for presentation at the 15th ACM Conference on Computer and Communications Security (CCS 2008), held October 27 to October 31, 2008 in Alexandria, VA, USA.

In response to the call for papers 280 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 four 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, 51 were selected for presentation at the conference, yielding in 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 are also very grateful to all other CCS 2008 organizers and the members of the CCS Steering Committee, 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.

Paul Syverson

CCS 2008 Program Chair

Somesh Jha

CCS 2008 Program Chair

Table of Contents

CCS 2008 Conference Organization	ix
CCS 2008 Additional Reviewers	xii
CCS 2008 Sponsors & Supporters.....	xiv

Keynote

Session Chair: Paul Syverson (*Naval Research Laboratory*)

- **The Good, the Bad, and the Provable.....** 1
Martín Abadi (*University of California, Santa Cruz and Microsoft Research*)

Session 1: Attacks 1

Session Chair: Michael Reiter (*University of North Carolina at Chapel Hill*)

- **Spamalytics: An Empirical Analysis of Spam Marketing Conversion.....** 3
Chris Kanich (*University of California at San Diego*),
Christian Kreibich (*International Computer Science Institute*),
Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker (*University of California at San Diego*),
Vern Paxson (*International Computer Science Institute*),
Stefan Savage (*University of California at San Diego*)
- **Code Injection Attacks on Harvard-Architecture Devices** 15
Aurélien Francillon, Claude Castelluccia (*INRIA Rhône-Alpes*)
- **When Good Instructions Go Bad: Generalizing Return-Oriented Programming to RISC.....** 27
Erik Buchanan, Ryan Roemer, Hovav Shacham, Stefan Savage (*University of California at San Diego*)

Session 2: Software Security 1

Session Chair: Mihai Christodorescu (*IBM Research, USA*)

- **Efficient and Extensible Security Enforcement Using Dynamic Data Flow Analysis.....** 39
Walter Chang, Brandon Streiff, Calvin Lin (*The University of Texas at Austin*)
- **Ether: Malware Analysis via Hardware Virtualization Extensions.....** 51
Artem Dinaburg (*Georgia Institute of Technology and Damballa, Inc.*),
Paul Royal (*Damballa Inc. and Georgia Institute of Technology*),
Monirul Sharif (*Georgia Institute of Technology and Damballa, Inc.*),
Wenke Lee (*Damballa Inc. and Georgia Institute of Technology*)
- **Extending Logical Attack Graphs for Efficient Vulnerability Analysis.....** 63
Diptikalyan Saha (*Motorola India Research Laboratory*)

Session 3: Browser Security

Session Chair: Xiaofeng Wang (*Indiana University*)

- **Robust Defenses for Cross-Site Request Forgery** 75
Adam Barth, Collin Jackson, John C. Mitchell (*Stanford University*)
- **SOMA: Mutual Approval for Included Content in Web Pages.....** 89
Terri Oda, Glenn Wurster, P. C. van Oorschot, Anil Somayaji (*Carleton University*)
- **OMash: Enabling Secure Web Mashups via Object Abstractions** 99
Steven Crites, Francis Hsu, Hao Chen (*University of California at Davis*)

Session 4: Formal Methods 1

Session Chair: Anupam Datta (*Carnegie Mellon University*)

- **Computational Soundness of Observational Equivalence.....** 109
Hubert Comon-Lundh (*Research Center for Information Security and ENS Cachan*),
Véronique Cortier (*LORIA, CNRS & INRIA*)

- **Unbounded Verification, Falsification, and Characterization of Security Protocols by Pattern Refinement** 119
Cas J. F. Cremers (*ETH Zurich*)
- **Reducing Protocol Analysis with XOR to the XOR-free Case in the Horn Theory Based Approach** 129
Ralf Küsters, Tomasz Truderung (*Universitaet Trier*)

Session 5: Privacy 1

Session Chair: George Danezis (*Microsoft Research Cambridge*)

- **Building Castles Out of Mud: Practical Access Pattern Privacy and Correctness on Untrusted Storage** 139
Peter Williams, Radu Sion (*Stony Brook University*), Bogdan Carbunar (*Motorola Laboratories*)
- **Location Privacy of Distance Bounding Protocols** 149
Kasper Bonne Rasmussen, Srdjan Čapkun (*ETH Zurich*)

Session 6: Software Security 2

Session Chair: Vinod Ganapathy (*Rutgers University*)

- **Verifiable Functional Purity in Java** 161
Matthew Finifter, Adrian Mettler, Naveen Sastry, David Wagner (*University of California, Berkeley*)
- **Trust Management for Secure Information Flows** 175
Mudhakar Srivatsa (*IBM T.J. Watson Research Center*),
Shane Balfé, Kenneth G. Paterson (*University of London*),
Pankaj Rohatgi (*IBM T.J. Watson Research Center*)

Session 7: Network Security

Session Chair: Paul Van Oorschot (*Carleton University*)

- **Mitigating DNS DoS Attacks** 189
Hitesh Ballani, Paul Francis (*Cornell University*)
- **Revocation Games in Ephemeral Networks** 199
Maxim Raya, Mohammad Hossein Manshaei (*EPFL*), Márk Félegyházi (*University of California, Berkeley*),
Jean-Pierre Hubaux (*EPFL*)
- **Increased DNS Forgery Resistance Through 0x20-Bit Encoding** 211
David Dagon, Manos Antonakakis (*Georgia Institute of Technology*),
Paul Vixie, Tatuya Jinmei (*Internet Systems Consortium*), Wenke Lee (*Georgia Institute of Technology*)

Session 8: System Security 1

Session Chair: Wenke Lee (*Georgia Institute of Technology*)

- **Enforcing Authorization Policies Using Transactional Memory Introspection** 223
Arnar Birgisson (*Reykjavik University*), Mohan Dhawan (*Rutgers University*),
Úlfar Erlingsson (*Reykjavik University*), Vinod Ganapathy, Liviu Iftode (*Rutgers University*)
- **Towards Practical Biometric Key Generation with Randomized Biometric Templates** 235
Lucas Ballard (*Google, Inc.*), Seny Kamara (*Microsoft Research*),
Fabian Monrose, Michael K. Reiter (*University of North Carolina at Chapel Hill*)
- **Towards Automatic Reverse Engineering of Software Security Configurations** 245
Rui Wang (*Indiana University*), XiaoFeng Wang (*Indiana University*),
Kehuan Zhang (*Indiana University and Hunan University*), Zhuowei Li (*Microsoft*)

Session 9: Privacy 2

Session Chair: Patrick McDaniel (*The Pennsylvania State University*)

- **FairplayMP — A System for Secure Multi-Party Computation** 257
Assaf Ben-David (*The Hebrew University*), Noam Nisan (*Google Tel Aviv and The Hebrew University*),
Benny Pinkas (*University of Haifa*)

- **Information Leaks in Structured Peer-to-Peer Anonymous Communication Systems**267
Prateek Mittal, Nikita Borisov (*University of Illinois at Urbana-Champaign*)
- **Privacy Oracle:
A System for Finding Application Leaks with Black Box Differential Testing**.....279
Jaeyeon Jung, Anmol Sheth, Ben Greenstein, David Wetherall (*Intel Research*),
Gabriel Maganis, Tadayoshi Kohno (*University of Washington*)

Session 10: Access Control

Session Chair: Ting Yu (*North Carolina State University*)

- **A Formal Framework for Reflective Database Access Control Policies**289
Lars E. Olson, Carl A. Gunter, P. Madhusudan (*University of Illinois at Urbana-Champaign*)
- **A Class of Probabilistic Models for Role Engineering**299
Mario Frank, David Basin, Joachim M. Buhmann (*ETH Zurich*)
- **Assessing Query Privileges via Safe and Efficient Permission Composition**.....311
Sabrina De Capitani di Vimercati, Sara Foresti (*Università di Milano*),
Sushil Jajodia (*George Mason University*), Stefano Paraboschi (*Università di Bergamo*),
Pierangela Samarati (*Università di Milano*)

Session 11: Anonymity

Session Chair: Aaron Johnson (*Yale University*)

- **Dependent Link Padding Algorithms for Low Latency Anonymity Systems**.....323
Wei Wang, Mehul Motani (*National University of Singapore*),
Vikram Srinivasan (*Bell Labs Research, India*)
- **PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication**333
Patrick P. Tsang (*Dartmouth College*), Man Ho Au (*University of Wollongong*),
Apu Kapadia, Sean W. Smith (*Dartmouth College*)
- **Efficient Attributes for Anonymous Credentials**.....345
Jan Camenisch, Thomas Groß (*IBM Research, Zurich Research Laboratory*)

Session 12: Formal Methods 2

Session Chair: Aaron Cédric Fournet (*Microsoft Research Cambridge*)

- **Type-Checking Zero-Knowledge**.....357
Michael Backes (*Saarland University and MPI-SWS*), Cătălin Hrițcu, Matteo Maffei (*Saarland University*)
- **Towards Automated Proofs for Asymmetric Encryption
Schemes in the Random Oracle Model**.....371
Judicaël Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, Yassine Lakhnech
(*Université Grenoble I, CNRS, Verimag*)
- **EON: Modeling and Analyzing Dynamic Access
Control Systems with Logic Programs**381
Avik Chaudhuri (*University of California at Santa Cruz*),
Prasad Naldurg, Sriram K. Rajamani, G. Ramalingam (*Microsoft Research India*),
Lakshmisubrahmanyam Velaga (*Indian Institute of Management*)

Session 13: System Security 2

Session Chair: Radu Sion (*Stonybrook University*)

- **Tupni: Automatic Reverse Engineering of Input Formats**391
Weidong Cui (*Microsoft Research*), Marcus Peinado (*Microsoft Corporation*),
Karl Chen (*University of California at Berkeley*),
Helen J. Wang, Luis Irun-Briz (*Microsoft Corporation*)
- **Rootkit-Resistant Disks**403
Kevin R. B. Butler, Stephen McLaughlin, Patrick D. McDaniel (*Pennsylvania State University*)

Session 14: Identity-Based Encryption

Session Chair: Steven Myers (*Indiana University*)

- **Identity-based Encryption with Efficient Revocation**417
Alexandra Boldyreva (*Georgia Institute of Technology*),
Vipul Goyal (*University of California at Los Angeles*), Virendra Kumar (*Georgia Institute of Technology*)
- **Black-Box Accountable Authority Identity-Based Encryption**427
Vipul Goyal, Steve Lu, Amit Sahai (*University of California at Los Angeles*),
Brent Waters (*University of Texas at Austin*)

Session 15: Applied Cryptography 1

Session Chair: Philippe Golle (*Palo Alto Research Center*)

- **Authenticated Hash Tables**.....437
Charalampos Papamanthou, Roberto Tamassia (*Brown University*),
Nikos Triandopoulos (*University of Aarhus*)
- **Multisignatures Secure under the Discrete Logarithm Assumption and a Generalized Forking Lemma**.....449
Ali Bagherzandi (*University of California at Irvine*), Jung-Hee Cheon (*Seoul National University*),
Stanislaw Jarecki (*University of California at Irvine*)
- **Cryptographically Verified Implementations for TLS**459
Karthikeyan Bhargavan, Cédric Fournet (*Microsoft Research Cambridge*),
Ricardo Corin, Eugen Zălinescu (*MSR-INRIA Joint Centre*)

Session 16: Device Security

Session Chair: J. Alex Halderman (*Princeton University*)

- **Reconsidering Physical Key Secrecy: Teleduplication via Optical Decoding**.....469
Benjamin Laxton, Kai Wang, Stefan Savage (*University of California at San Diego*)
- **RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications**479
Alexei Czeskis, Karl Koscher (*University of Washington*), Joshua R. Smith (*Intel Research Seattle*),
Tadayoshi Kohno (*University of Washington*)
- **Constructions of Truly Practical Secure Protocols Using Standard Smartcards**491
Carmit Hazay, Yehuda Lindell (*Bar-Ilan University*)

Session 17: Applied Cryptography 2

Session Chair: Catherine Meadows (*Naval Research Laboratory*)

- **Traitor Tracing with Constant Size Ciphertext**.....501
Dan Boneh (*Stanford University*), Moni Naor (*Weizmann Institute of Science*)
- **Multi-Use Unidirectional Proxy Re-Signatures**511
Benoît Libert (*Université Catholique de Louvain*), Damien Vergnaud (*Ecole Normale Supérieure*)
- **Efficient Security Primitives Derived from a Secure Aggregation Algorithm**521
Haowen Chan, Adrian Perrig (*Carnegie Mellon University*)

Session 18: Attacks 2

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

- **Machine Learning Attacks Against the Asirra CAPTCHA**.....535
Philippe Golle (*Palo Alto Research Center*)
- **A Low-cost Attack on a Microsoft CAPTCHA**543
Jeff Yan, Ahmad Salah El Ahmad (*Newcastle University*)
- **BootJacker: Compromising Computers Using Forced Restarts**555
Ellick M. Chan, Jeffrey C. Carlyle, Francis M. David, Reza Farivar, Roy H. Campbell
(*University of Illinois at Urbana-Champaign*)
- **A Look In the Mirror: Attacks on Package Managers**565
Justin Cappos, Justin Samuel, Scott Baker, John H. Hartman (*University of Arizona*)

Author Index.....575

CCS 2008 Conference Organization

- General Chair:** Peng Ning (*North Carolina State University, USA*)
- Program Chairs:** Paul Syverson (*Naval Research Laboratory, USA*)
Somesh Jha (*University of Wisconsin, USA*)
- Tutorials Chair:** Pierangela Samarati (*University of Milan, Italy*)
- Publicity Chair:** Radha Poovendran (*University of Washington, USA*)
- Publication Chair:** Xiaolan Zhang (*IBM T.J. Watson Research Center, USA*)
- Web Chair:** Ting Yu (*North Carolina State University, USA*)
- Treasurer:** Sencun Zhu (*The Pennsylvania State University, USA*)
- Workshops Chair:** Vijay Atluri (*Rutgers University, USA*)
- Steering Committee:** Carl A. Gunter (Chair) (*University of Illinois at Urbana-Champaign, USA*)
Peng Ning (*North Carolina State University, USA*)
Pierangela Samarati (*University of Milan, Italy*)
Paul Syverson (*Naval Research Laboratory, USA*)
Gene Tsudik (*University of California, Irvine, USA*)
Moti Yung (*Google & Columbia University, USA*)
- Program Committee:** Martín Abadi (*UC Santa Cruz & Microsoft Research, USA*)
Ben Adida (*Harvard University, USA*)
Mikhail Atallah (*Purdue University, USA*)
Giuseppe Ateniese (*The Johns Hopkins University, USA*)
Vijay Atluri (*Rutgers University, USA*)
Paul Barford (*University of Wisconsin, USA*)
Nikita Borisov (*University of Illinois at Urbana-Champaign, USA*)
L. Jean Camp (*Indiana University, USA*)
Ilario Cervesato (*Carnegie Mellon University, Qatar*)
Ajay Chander (*DOCOMO USA Labs, USA*)
Mihai Christodorescu (*IBM Research, USA*)
Richard Clayton (*University of Cambridge, UK*)
Lorrie Cranor (*Carnegie Mellon University, USA*)
Marco Cremonini (*University of Milan, Italy*)
George Danezis (*Microsoft Research Cambridge, UK*)
Anupam Datta (*Carnegie Mellon University, USA*)
Sabrina De Capitani di Vimercati (*University of Milan, Italy*)
Robert Deng (*Singapore Management University, Singapore*)
Claudia Diaz (*K.U.Leuven, Belgium*)
Sven Dietrich (*Stevens Institute of Technology, USA*)

Program Committee

(continued): Wenliang (Kevin) Du (*Syracuse University, USA*)
Matt Edman (*Rensselaer Polytechnic Institute, USA*)
Dawson Engler (*Stanford University, USA*)
Nick Feamster (*Georgia Institute of Technology, USA*)
Simone Fischer-Huebner (*Karlstad University, Sweden*)
Jeff Foster (*University of Maryland, College Park, USA*)
Cédric Fournet (*Microsoft Research Cambridge, UK*)
Michael Freedman (*Princeton University, USA*)
Vinod Ganapathy (*Rutgers University, USA*)
Eu-Jin Goh (*Stanford University, USA*)
Philippe Golle (*Palo Alto Research Center, USA*)
Rachel Greenstadt (*Drexel University, USA*)
Steven Gribble (*University of Washington, USA*)
J. Alex Halderman (*Princeton University, USA*)
Michael Hicks (*University of Maryland, College Park, USA*)
Trent Jaeger (*The Pennsylvania State University, USA*)
Farnam Jahanian (*University of Michigan, USA*)
Aaron Johnson (*Yale University, USA*)
Rob Johnson (*Stony Brook University, USA*)
Ari Juels (*RSA Laboratories, USA*)
Angelos Keromytis (*Columbia University, USA*)
Tadayoshi Kohno (*University of Washington, USA*)
Christopher Kruegel (*University of California, Santa Barbara, USA*)
Wenke Lee (*Georgia Institute of Technology, USA*)
Brian Levine (*University of Massachusetts Amherst, USA*)
Ninghui Li (*Purdue University, USA*)
Peng Liu (*The Pennsylvania State University, USA*)
Heiko Mantel (*TU Darmstadt, Germany*)
Z. Morley Mao (*University of Michigan, USA*)
Nick Mathewson (*The Tor Project, USA*)
Patrick McDaniel (*The Pennsylvania State University, USA*)
Catherine Meadows (*Naval Research Laboratory, USA*)
John C. Mitchell (*Stanford University, USA*)
David Molnar (*University of California, Berkeley, USA*)
James Muir (*Cloakware, Canada*)
Steven Murdoch (*University of Cambridge, UK*)
Steven Myers (*Indiana University, USA*)
Prasad Naldurg (*Microsoft Research, India*)
Peng Ning (*North Carolina State University, USA*)
Cristina Nita-Rotaru (*Purdue University, USA*)
Lasse Øverlier (*Norwegian Defence Research Establishment, Norway*)
Stefano Paraboschi (*University of Bergamo, Italy*)
Adrian Perrig (*Carnegie Mellon University, USA*)
Andreas Pfitzmann (*Dresden University of Technology, Germany*)

Program Committee

(continued): Bart Preneel (*K.U. Leuven, Belgium*)
Sriram Rajamani (*Microsoft Research, India*)
Michael K. Reiter (*University of North Carolina at Chapel Hill, USA*)
Andrei Sabelfeld (*Chalmers University of Technology, Sweden*)
Kazue Sako (*NEC, Japan*)
Pierangela Samarati (*University of Milan, Italy*)
Andre Scedrov (*University of Pennsylvania, USA*)
Steve Schneider (*University of Surrey, UK*)
Hovav Shacham (*University of California, San Diego, USA*)
Umesh Shankar (*Google, USA*)
Shiuhpyng Shieh (*National Chiao Tung University, Taiwan*)
Vitaly Shmatikov (*University of Texas at Austin, USA*)
Radu Sion (*Stony Brook University, USA*)
Anil Somayaji (*Carleton University, Canada*)
Jessica Staddon (*Palo Alto Research Center, USA*)
Salvatore Stolfo (*Columbia University, USA*)
Michael Swift (*University of Wisconsin, USA*)
Julie Thorpe (*Carleton University, Canada*)
Paul Van Oorschot (*Carleton University, Canada*)
Giovanni Vigna (*University of California, Santa Barbara, USA*)
Dan Wallach (*Rice University, USA*)
Helen Wang (*Microsoft Research, USA*)
Xiaofeng Wang (*Indiana University, USA*)
Nicholas Weaver (*International Computer Science Institute, USA*)
Marianne Winslett (*University of Illinois at Urbana-Champaign, USA*)
Rebecca Wright (*Rutgers University, USA*)
Alec Yasinsac (*Florida State University, USA*)
Ting Yu (*North Carolina State University, USA*)
Jianying Zhou (*Institute for Infocomm Research, Singapore*)

CCS 2008 Additional Reviewers

Pedro Adão	Brian Corcoran	Keith Irwin
David Albrecht	Ricardo Corin	Toshiyuki Isshiki
Jacob Appelbaum	Véronique Cortier	Collin Jackson
Toshinori Araki	Marco Cova	Mariusz Jakubowski
Claudio A. Ardagna	Weidong Cui	Karthick Jayaraman
Aslan Askarov	Reza Curtmola	Yoon-Chan Jhi
Kumar Avijit	Alexei Czeskis	Tao Jiang
Eric Bach	Rob Delicata	Thomas Johansson
Joonsang Baek	Dinakar Dhurjati	Jaeyeon Jung
Kun Bai	Xuhua Ding	Chris Karlof
Daniel Bailey	Roger Dingledine	Emilia Käsper
Michael Bailey	William Enck	Dilsun Kaynar
Arati Baliga	Santiago Escobar	David H. King
Davide Balzarotti	Nelly Fazio	Darko Kirovski
Sruthi Bandhakavi	Ariel Feldman	Lea Kissner
Adam Barth	Viktorya Felmetsger	Negar Kiyavash
Lejla Batina	Anna Lisa Ferrara	Markulf Kohlweiss
Lujo Bauer	Jeffrey Fischer	Vladimir Kolesnikov
Mike Bergmann	Sara Foresti	Karl Koscher
John Bethencourt	Jason Franklin	Kameswari Kotapati
Karthikeyan Bhargavan	Elke Franz	Louis Kruger
Raghav Bhaskar	Matt Fredrickson	Markus G. Kuhn
George Bissias	Vanessa Frias-Martinez	Klaus Kursawe
Michael Black	Keith Frikken	Stefan Köpsell
Bruno Blanchet	Jun Furukawa	Adam J. Lee
Brian Bowen	Debin Gao	Lunquan Li
Xavier Boyen	Deepak Garg	Zhuowei Li
Justin Brickell	Jonathon Giffin	Hsiao-Ying Lin
Niklas Broberg	Thomas Gloe	Joseph Liu
Kevin Butler	Sharon Goldberg	Michael Locasto
Rainer Böhme	Jean Goubault-Larrecq	Alexander Lux
Joseph Calandrino	Matthew Green	Xiaonan Ma
Bogdan Carbunar Carbunar	Ben Greenstein	Sergio Maffei
Pavol Cerny	Benjamin Grégoire	Ziqing Mao
Sagar Chaki	Chris Grier	Leonardo Martucci
Haowen Chan	Stephan Groß	Brendon D. Mayes
Shuo Chen	Qijun Gu	Damon McCoy
Hong Chen	Helen (Xiaohui) Gu	Jon McCune
Richard Chow	Ragib Hasan	Kazuhiro Minami
Andrey Chudnov	Hans Hedbom	Ilya Mironov
Sebastian Clauß	Amir Houmansadr	Soumyadeb Mitra
Robert Cole	Sebastiaan Indestege	Ian Molloy

David Molnar	Dries Schellekens	Vilhelm Verendel
Tyler Moore	Joshua Schiffman	Hayawardh Vijayakumar
Kengo Mori	Immanuel Scholz	Qihua Wang
Divya Muthukumaran	Dieter Schuster	Guan Wang
Arvind Narayanan	Siraj Shaikh	Rui Wang
Iulian Neamtiu	Jun Shao	Gary Wassermann
Gene Novark	Monirul Sharif	Robert N.M. Watson
Kautubh Nyalkalkar	Elaine Runting Shi	Jian Weng
Jon Oberheide	YoungSang Shin	Andreas Westfeld
Lars Olson	Jeff Siebert	Peter Williams
Alina Oprea	Koen Simoens	Tilman Wolf
Valeria de Paiva	Sushant Sinha	Edmund Wong
Martin Paraskevov	Yingbo Song	Hao-Chi Wong
Bryan Parno	Barbara Sprick	Zhe Xia
Cem Paya	Sukamol Srikwan	Ji Xiang
Bryan Payne	Sid Stamm	Xi Xiong
Gerardo Pelosi	Sandra Steinbrecher	Haizhi Xu
Christine Pepin	Paul Stewart	Bo-Yin Yang
Carlos-Rene Perez	Scott Stoller	Yanjiang Yang
Nick L. Petroni, Jr.	Ahren Studer	Ting-Fang Yen
Benjamin Pflanz	Henning Sudbrock	Scott Yilek
Polyvios Pratikakis	Nikhil Swamy	Meng Yu
Ning Qu	Isamu Teranishi	Eugen Zalinescu
Raghavendra K R	Arash Termehchy	Wanyu Zang
Svetlana Radosavac	Patrick Traynor	Bill Zeller
Charlie Reis	Helen Treharne	Qing Zhang
Eric Rescorla	Carmela Troncoso	Kehuan Zhang
Patrick Reynolds	Michael Carl Tschantz	Charles Zhang
Mike Rosulek	Christina Tziviskou	Ge Zhang
Sandra Rueda	Yevgeniy Vahlis	
Amirali Salehi-Abari	Jaideep Vaidya	
Thierry Sans	Amit Vasudevan	
Len Sassaman	Shobha Venkataraman	
Nabil Schear	Frederik Vercauteren	

CCS 2008 Sponsor & Supporters

Sponsor:



Supporters:



Dartmouth College
**INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES**

Google

IBM Research

Microsoft®
Research

