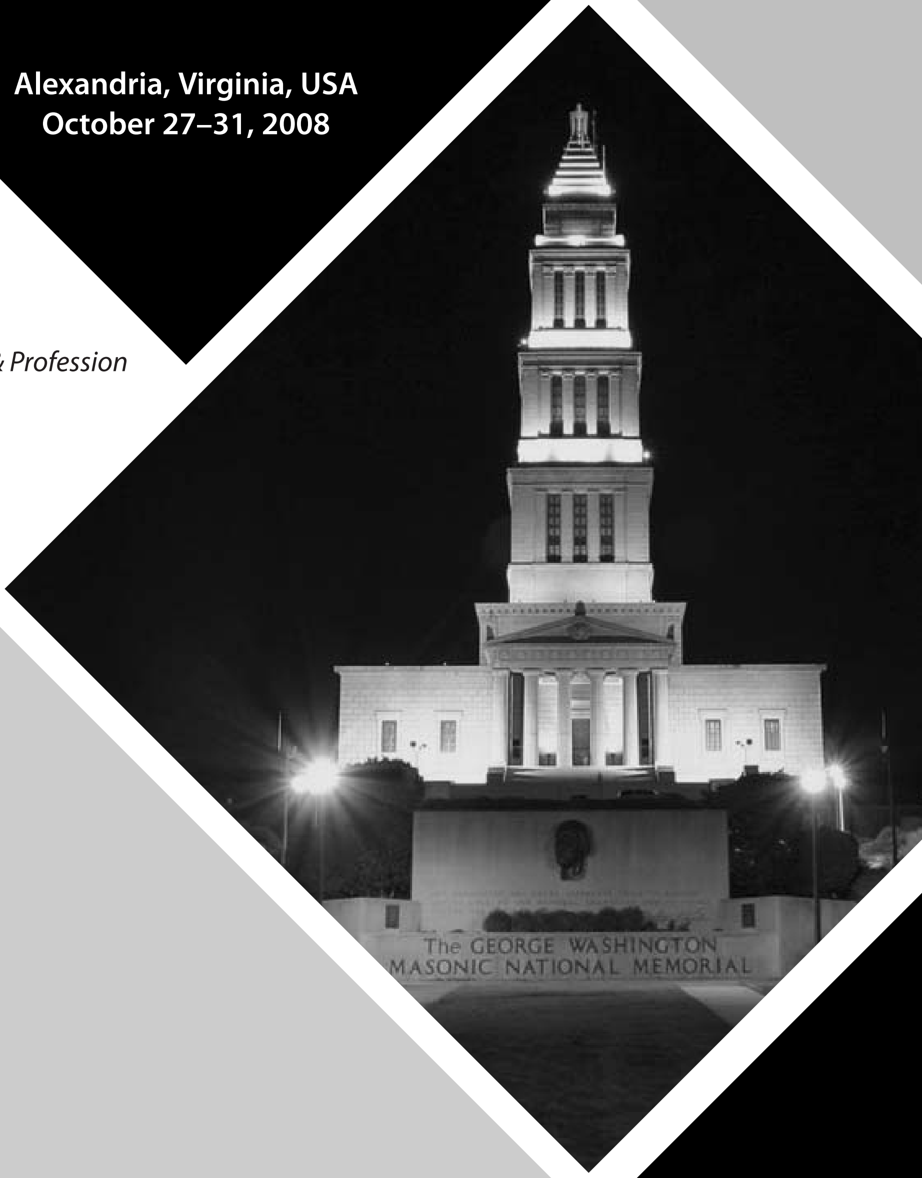
Alexandria, Virginia, USA
October 27–31, 2008

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

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 Stavrous (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

Keynote

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

Session 1: Attacks 1

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

Session 2: Software Security 1

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

Session 3: Browser Security

Session Chair: Xiaofeng Wang *(Indiana University)*

Session 4: Formal Methods 1

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

Session 5: Privacy 1

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

Session 6: Software Security 2

Session Chair: Vinod Ganapathy *(Rutgers University)*

Session 7: Network Security

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

Session 8: System Security 1

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

Session 9: Privacy 2

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

Session 10: Access Control

Session 11: Anonymity

Session 12: Formal Methods 2

Session 13: System Security 2

Session 14: Identity-Based Encryption

Session Chair: Steven Myers *(Indiana University)*

Session 15: Applied Cryptography 1

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

Session 16: Device Security

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

Session 17: Applied Cryptography 2

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

Session 18: Attacks 2

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

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

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

CCS 2008 Sponsor & Supporters

Sponsor:

acm
SIGSAC

Supporters:

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES

Google

IBM Research

Microsoft®
Research

MOTOROLA