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

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

Session 5: Traffic Analysis and Location Privacy

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

Session 6: Cryptography

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

Session 7: Network Security

Session Chair: Rachel Greenstadt *(Harvard University)*

Session 8: Election Systems and Applied Cryptography

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

Session 9: Side and Covert Channels Detection

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

Session 10: Protocols and Spam Filters

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

Session 11: Internet Security

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

Session 12: Key Management

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

Session 13: Policies

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

Session 14: Cryptography and Cryptoanalysis

Session Chair: Ari Juels *(RSA Laboratories)*

Session 15: Data Privacy

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

Session 16: Software Security

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

Session 17: Data Disclosure

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

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

Additional reviewers (continued):

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

Sponsor:

Supporters:

IBM Research

Microsoft®
Research