CCS 2006

Proceedings of the 13th ACM Conference on Computer and Communications Security

October 30-November 3, 2006 • Alexandria, Virginia, USA

Sponsored by

ACM Special Interest Group on Security, Audit & Control

Rebecca N. Wright, Sabrina De Capitani di Vimercati, & Vitaly Shmatikov, *Editors*

The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York, New York 10121-0710

ISBN: 1-59593-518-5

Additional copies may be ordered prepaid from:

ACM Order Department
General Post Office
P.O. Box 30777
New York, NY 10087-0777

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 537060
Printed in the USA

Welcome to CCS 2006

It is a pleasure and honor to welcome you to the *13th 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 a research track, an industry track, three tutorials, and eleven 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 Rebecca Wright and Sabrina De Capitani di Vimercati, the research-track program chair and co-chair respectively, 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, Peter Dinsmore, and his program committee for arranging talks on applied topics to complement the other conference offerings.

I would like to extend my appreciation to Marianne Winslett, 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: Kaoru Kurosawa and Rei Safavi-Naini (Workshop on Digital Rights Management); Donggang Liu and Sencun Zhu (Workshop on Security of Ad Hoc and Sensor Networks); Roger Dingledine and Ting Yu (Workshop on Privacy in Electronic Society); Guenter Karjoth and Fabio Massacci **(**Workshop on Quality of Protection); Ethan Miller and Erez Zadok (Workshop on Storage Security and Survivability); Farnam Jahanian (Workshop on Recurring Malcode); Andrew D. Gordon and David Sands (Workshop on Formal Methods in Security Engineering: From Specifications to Code); Stefan Axelsson, Kiran Lakkaraju, Soon Tee Teoh, and Bill Yurcik (Workshop on Visualization for Computer Security); Gene Tsudik, Shouhuai Xu, and Moti Yung (Workshop on Scalable Trusted Computing); Atsuhiro Goto (Workshop on Digital Identity Management); and Ernesto Damiani and Alban Gabillon (Workshop on Secure Web Services). In the past two years, the conference has expanded its program of satellite workshops from six to eleven. I would also like to express my thanks to Wenliang (Kevin) Du for a strong program of tutorials.

I am grateful to Peter Neumann for delivering the keynote address. My thanks as well to those who have offered their untiring administrative support, namely to Peng Ning for managing the budget, Vitaly Shmatikov for assisting with the preparation of the proceedings, and Michael Locasto and Angelos Keromytis their joint work as publicity chairs. 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.

Finally, I wish to thank the following institutions for their generous sponsorship: The Defense Advanced Research Projects Agency, The Army Research Office, and IBM 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.

Ari Juels
General Chair
ACM CCS 2006

Message from the Program Chairs

We are delighted to join Ari Juels in welcoming you to the *13th ACM Conference on Computer and Communications Security*, held October 30 to November 3, 2006 at the Hilton Alexandria Mark Center, Alexandria, Virginia, USA. These proceedings contain 38 papers presented in the research track and a paper contributed by our keynote speaker, Peter Neumann. The conference also comprises an industry track, tutorials, and workshops.

The 38 research track papers contained in this proceedings were selected from 256 received submissions. These submissions were carefully reviewed by at least three members of the program committee, or four in the case of papers authored by program committee members. 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. Program committee members were allowed to use external reviewers, but were responsible for the contents of the review and representing papers during the decision making. The review phase was followed by a three-week discussion phase in which each paper with at least one supporting review was discussed, outside experts were consulted where needed, and final decisions were made.

We thank the program committee for their hard work in selecting the program from these papers. We also thank the external referees that helped with the reviewing task and Cathy Meadows for providing helpful advice based on her experience as CCS'05 program chair. We thank the CCS steering committee and other CCS'06 organizers for their help, which allowed us to focus on putting together the research program. We also thank Thomas Herlea for running the WebReview system that was used for the electronic submission and review of the submitted papers.

Finally, we thank all authors who submitted papers and all conference attendees. Without them, there would be no conference.

Rebecca Wright
CCS 2006 Research Track
Program Chair

Sabrina De Capitani di Vimercati
CCS 2006 Research Track
Program Co-Chair

Table of Contents

Session 5: Privacy and Authentication

Session Chair: R. Safavi-Naini *(University of Wollongong)*

Session 6: Applied Cryptography I

Session Chair: M. Backes *(Saarland University)*

Session 7: Attacks and Cryptanalysis

Session Chair: P. Vora *(George Washington University)*

Session 8: Sensors and Networking

Session Chair: B. Levine *(University of Massachusetts at Amherst)*

Session 9: Software and Network Exploits

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

Session 10: Formal Methods

Session Chair: T. Yu *(North Carolina State University)*

Session 11: Applied Cryptography II

Session Chair: M. Goodrich *(University of California at Irvine)*

CCS 2006 Conference Organization

General Chair: Ari Juels *(RSA Laboratories, USA)*

Program Chair: Rebecca Wright *(Stevens Institute of Technology, USA)*

Program Co-Chair: Sabrina De Capitani di Vimercati *(University of Milan, Italy)*

Industry and Government Track Chair: Peter Dinsmore *(Johns Hopkins University Applied Physics Lab, USA)*

Publicity Chairs: Angelos Keromytis *(Columbia University, USA)*
Michael E. Locasto *(Columbia University, USA)*

Publication Chair: Vitaly Shmatikov *(The University of Texas at Austin, USA)*

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

Treasurer: Peng Ning *(North Carolina State University, USA)*

Workshops Chair: Marianne Winslett *(UIUC, USA)*

Program Committee: Carlisle Adams *(University of Ottawa, Canada)*
Giuseppe Ateniese *(Johns Hopkins University, USA)*
Vijay Atluri *(Rutgers University, USA)*
Michael Backes *(Saarland University, Germany)*
Giampaolo Bella *(Università di Catania, Italy)*
John Black *(University of Colorado, USA)*
Nikita Borisov *(UIUC, USA)*
Jan Camenisch *(IBM Research, Switzerland)*
Rosario Gennaro *(IBM T. J. Watson Research Center, USA)*
Michael Goodrich *(UC Irvine, USA)*
Stefanos Gritzalis *(University of the Aegean, Greece)*
Trent Jaeger *(Penn State University, USA)*
Markus Jakobsson *(Indiana University, USA)*
Somesh Jha *(University of Wisconsin, USA)*
Trevor Jim *(AT&T Research, USA)*
Jonathan Katz *(University of Maryland, USA)*
Brian Levine *(University of Massachusetts, Amherst, USA)*
Ninghui Li *(Purdue University, USA)*
Peng Liu *(Penn State University, USA)*
Javier Lopez *(University of Malaga, Spain)*
Patrick McDaniel *(Penn State University, USA)*
Catherine Meadows *(Naval Research Laboratory, USA)*

Program Committee (continued):

Nasir Memon *(Polytechnic University, USA)*
John Mitchell *(Stanford University, USA)*
Refik Molva *(Institut Eurecome, Sophia Antipolis, France)*
Eiji Okamoto *(University of Tsukuba, Japan)*
Phillip Porras *(SRI International, USA)*
Rei Safavi-Naini *(University of Wollongong, Australia)*
Reiner Sailer *(IBM T. J. Watson Research Center, USA)*
Pierangela Samarati *(Università degli Studi di Milano, Italy)*
Andre Scedrov *(University of Pennsylvania, USA)*
R. Sekar *(SUNY Stony Brook, USA)*
Shiuhpyng Shieh *(National Chiao Tung University, Taiwan)*
Sean Smith *(Dartmouth College, USA)*
Dawn Song *(Carnegie Mellon University, USA)*
Jessica Staddon *(Palo Alto Research Center, USA)*
Giovanni Vigna *(UC Santa Barbara, USA)*
Poorvi Vora *(George Washington University, USA)*
Susanne Wetzel *(Stevens Institute of Technology, USA)*
Shouhuai Xu *(University of Texas at San Antonio, USA)*
Alec Yasinsac *(Florida State University, USA)*
Ting Yu *(North Carolina State University, USA)*
Sheng Zhong *(SUNY Buffalo, USA)*

Sponsor:

Supporters:

IBM Research

External Reviewers

Fenia Aivaloglou
Soon Ae Chun
Isaac Agudo
Mansour Alsaleh
Kun Bai
Theodoros Balopoulos
Davide Balzarotti
Greg Banks
Lujo Bauer
Steve Bellovin
Petros Belsis
Abhilasha Bhargav-Spantzel
Sandeep Bhatkar
Christophe Bidan
Olivier Billet
George Bissias
Marina Blanton
Damiano Bolzoni
Xavier Boyen
Linda Briesemeister
Arslan Broemme
Kevin Butler
Mike Burmester
Ji-Won Byun
Christian Cachin
Ran Canetti
Alvaro Cardenas
Dario Catalano
Iliano Cervesato
Hong Chen
Mihai Christodorescu
Jeremy Clark
Richard Clayton
Martin Cochran
Robert Cole
Carine Courbis
Lorrie Cranor
Stefano Crosta
Frederic Cuppens
Reza Curtmola
Breno de Medeiros
Drew Dean
Jing Deng
Mario Di Raimondo
Wenliang Du
Markus Duermuth
Glenn Durfee
Aleks Essex
Jianping Fan
Siamak Fayyaz-Shahandashti
Nelly Fazio
Nick Feamster
Gerardo Fernandez
Maria C. Fernandez
Luca Foschini
Martin Gagne
Vinod Ganapathy
Dimitris Geneiatakis
Jonathan Giffin
Matthew Green
Guofei Gu
Qijun Gu
Lazaros Gymnopoulos
Shai Halevi
Keith Harrison
Susan Hohenberger
Jason Holt
Jeffrey Horton
John Iliadis
Sotiris Ioannidis
Keith Irwin
Yoon-Chan Jhi
Lisa Johansen
Rob Johnson
Marc Joye
Christos Kalloniatis
Yogesh Kalyani
Seny Kamara
George Kambourakis
Costas Karafasoulis
Paul Karger
Erhan Kartaltepe
Maria Karyda
Aggelos Kiayias
Yunhua Koglin
Spyros Kokolakis
Kameswari Kotapati
Louis Kruger
Costas Lambrinoudakis
Adam Lee
Corrado Leita
Chris Lesniewski-Laas
Dave Levin
Marc Liberatore
Fengjun Li
Jiangtao Li
Lunquan Li
Qiming Li
Tiancheng Li
Zhenkai Liang
Jiqiang Liu
Liang Lu
Bo Luo
Matteo Maffei
Ziqing Mao
Boris Margolin
Brad Metz
Mira Meyerovich
Pietro Michiardi
Gerome Miklau
Sebastian Moedersheim
Frédéric Montagut
Razvan Musaloiu-E.
Antonio Nicolosi
Jesper Buus Nielsen
Melek Önen
Aabhas Paliwal
Chi-Chun Pan
Paul Parker
Bryan D. Payne
Adrian Perrig
Marinella Petrocchi
Van Hau Pham

Angela Piper
Richard Qing
Wei Qiu
Michael Rabinovich
Vijay Ramachandran
Rodrigo Roman
Kurt Rosenfeld
Yves Roudier
Farzad Salim
Taha Sencar
Hovav Shacham
Kulesh Shanmugasundaram
Raman Sharykin
abhi shelat
Nicholas Sheppard
Clay Shields
Abdullatif Shikfa
Heechang Shin
Radu Sion
Randy Smith
Miguel Soriano
Sid Stamm
Michael Steiner
Adam Stubblefield
Weiqing Sun
Paul Syverson
Gelareh Taban
Parisa Tabriz
Andreas Terzis
Ashish Thapliyal
Bhavani Thuraisingham
Alok Tongaonkar
Slim Trabelsi
Patrick Traynor
Mahesh V. Tripunitara
Theodoros Tzouramanis
Tri van Le
V.N. Venkatakrishnan
Jose L. Vivas
David Wagner
Hai Wang
Hao Wang
Qihua Wang
Xiaofeng Wang
Janice Warner
Brent Waters
William H. Winsborough
Hoeteck Wee
David Woodruff
Fan Wu
Qianhong Wu
Xintao Wu
Yuqing Wu
Jun Xu
Wei Xu
Zhiqiang Yang
Stefano Zanero
Zhijun Zhan
Chengqiang Zhang
Qing Zhang
Li Zhuang