CCS 2004

CCS 2004

Proceedings of the 11th ACM Conference on Computer & Communications Security
October 25-29, 2004 • Washington, DC, USA

acm PRESS

# Proceedings of the
# 11th ACM Conference on Computer and Communications Security

## Washington, DC, USA • October 25-29, 2004

Edited by: Birgit Pfitzmann & Peng Liu

Sponsored by

acm SIGSAC

with contributions from

Defense Advanced Research Project Agency,
IBM Research, NTT DoCoMo, and U.S. Army Research Office

CCS 2004

# Proceedings of the
# 11th ACM Conference on Computer and Communications Security

## Washington, DC, USA • October 25-29, 2004

**Edited by: Birgit Pfitzmann & Peng Liu**

**Sponsored by**

ACM SIGSAC

**with contributions from**

**Defense Advanced Research Project Agency,**
**IBM Research, NTT DoCoMo, and U.S. Army Research Office**

**The Association for Computing Machinery**
**1515 Broadway**
**New York, New York 10036**



**ISBN:** 1-58113-961-6

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** 459040
Printed in the USA

# Welcome to CCS 2004

It is a pleasure and honor to welcome you to the *11th ACM Conference on Computer and Communications Security*. This year's conference will continue its tradition of being a premier forum for the presentation of results in security research. We have an excellent program comprising of the research track, industry track, seven workshops and three tutorials that cover a variety of interests and disciplines in the area of computer and communication security.

Many individuals have contributed to the success of the conference of this magnitude. First, I would like to thank Birgit Pfitzmann, the research track program chair, and the members of the program committee for selecting the papers in the research track. The standards for acceptance continued to remain high with an acceptance ratio of 35/251. Second, I would like to thank the industry track chair, Patrick McDaniel and the members of the industry program committee for putting together a fantastic program. Next, I would like to express my thanks to Ravi Sandhu for having excellent tutorials in this year's program.

I would like to extend my appreciation to Sushil Jajodia, the workshops chair, for putting together the very best workshops and ensuring the smooth running of them. I would like to thank all the workshop program chairs who helped organize these workshops, specifically: Aggelos Kiayias and Moti Yung (Workshop on Digital Rights Management); Sanjeev Setia and Vipin Swarup (Workshop on Security of Ad Hoc and Sensor Networks); Paul Syverson and Sabrina De Capitani di Vimercati (Workshop on Privacy in Electronic Society); Vern Paxon (Workshop on Rapid Malcode); Michael Backes, David Basin, and Michael Waidner (Workshop on Formal Methods in Security Engineering: From Specifications to Code); Hiroshi Maruyama and Ernesto Damiani (Workshop on Secure Web Services); and Carla Brodley, Philip Chan, Richard Lippmann and Bill Yurcik (Workshop on Visualization and Data Mining for Computer Security). While the first 5 of the 7 workshops are being organized for the second time since their introduction last year, the last two are new this year.

I am grateful to John McLean for agreeing to deliver the Conference keynote address, Peng Ning for managing the budget, Peng Liu for assisting with the preparation of the proceedings, and Gail-Joon Ahn for maintaining the web site and for taking care of the publicity. I would also like to acknowledge the administrative staff at the ACM headquarters and George Mason University for their support.

I wish to thank the following institutions for their generous financial support: Defense Advanced Research Projects Agency, The Army Research Office, IBM Research, and DoCoMo Communications Laboratories.

Last but not least, my thanks go to all the authors who submitted papers and all the attendees. I hope you find the CCS and the workshop programs stimulating and beneficial for your research. Welcome and enjoy the conference.

**Vijay Atluri**
*General Chair*

# Program Chair's Message

I am delighted to join Vijay Atluri in welcoming you to the *11th ACM Conference on Computer and Communications Security*, held Oct 25-29, 2004 at the Wyndham City Center Hotel, Washington, DC, USA. These proceedings contain the papers presented at the research track. This track is surrounded by a keynote speech, an industry track, tutorial, and workshops.

The present papers were selected from 251 submissions on all areas of information security from authors worldwide. Submissions had been invited with the only restriction that theoretical papers must demonstrate the practical significance of the results. The selected papers were chosen on the basis of excellence of scientific contribution by a program committee of 53 experts. Each paper was assigned for review to 3 program committee members, or 5 for papers by committee members or with other potential conflicts of interest. They were evaluated on the criteria of scientific novelty, importance to the field, and technical quality. The authors did not know the identities of the reviewers, and the reviewers did not know the identity of the authors and had no known relation to the authors. In some cases advice was sought from colleagues outside the committee. Initial independent reviews were followed by intensive web-based discussions. The final selection of papers for the conference took place in four telephone conferences for different subject areas.

I am grateful for the efforts of the members of the Program Committee and the outside reviewers, and also to the many authors who submitted papers. A great deal of hard work goes into generating a quality program, not least by the many authors whose papers did not quite make it. We hope that all authors who submitted papers have found the reviewers' comments helpful.

My particular thanks go to my colleague Roger Zimmermann for running the submission and reviewing servers, Vijay Atluri and Sushil Jajodia, last year's program chair and the chair of the steering committee, for their support and suggestions, and Peng Liu and Gail-John Ahn, the proceedings chair and publicity chair, for smoothly freeing me of most administrational tasks of making a program real.

We all hope that you will find the program stimulating. We are looking forward to your comments and discussions at the conference, which will be another major contribution to the success of the conference.

**Birgit Pfitzmann**
*CCS 2004 Program Chair*

# Table of Contents

## Session 7: Information flow



## Session 8: Privacy



## Session 9: Puzzles and users



## Session 10: Applications of formal methods



## Session 11: Operating systems security

## Session 12: Cryptographic tools

# CCS 2004 Conference Organization

**General Chair:** Vijay Atluri, *Rutgers University, USA*

**Program Chair (Research Track):** Birgit Pfitzmann, *IBM Research, Switzerland*

**Program Chair (Industry Track):** Patrick McDaniel, *Pennsylvania State University, USA*

**Tutorials Chair:** Ravi Sandhu, *George Mason University, USA*

**Workshops Chair:** Sushil Jajodia, *George Mason University, USA*

**Proceedings Chair:** Peng Liu, *Pennsylvania State University, USA*

**Publicity Chair:** Gail-Joon Ahn, *University of North Carolina at Charlotte, USA*

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

**Steering Committee:**
Sushil Jajodia (Chair), *George Mason University, USA*
Ravi Ganesan, *SingleSignOn.Net & NSD Security, USA*
Ravi Sandhu, *George Mason University and NSD Security, USA*
Pierangela Samarati, *University of Milan, Italy*

**Program Committee:**
Paul Ammann, *George Mason University, USA*
David Basin, *ETH Zurich, Switzerland*
Birgit Baum-Waidner, *IBM Research, Switzerland*
Elisa Bertino, *Università di Milano, Italy and Purdue University, USA*
Piero Bonatti, *Università di Napoli, Italy*
Marc Dacier, *Eurécom, France*
Sabrina De Capitani di Vimercati, *Università di Milano, Italy*
Drew Dean, *SRI, USA*
Hervé Debar, *France Telecom R&D, France*
Hannes Federrath, *Universität Regensburg, Germany*
Matthias Fitzi, *University of California, Davis, USA*
Simon Foley, *University College Cork, Ireland*
Yair Frankel, *TechTegrity, USA*
Juan Garay, *Bell Labs - Lucent Technologies, USA*
Hugo Krawczyk, *Technion, Israel & IBM Research, USA*
Markus Kuhn, *University of Cambridge, UK*
Helmut Kurth, *Atsec Information Security, Germany*
Brian LaMacchia, *Microsoft, USA*
Peeter Laud, *Tartu University, Estonia*
Ninghui Li, *Purdue University, USA*
Helger Lipmaa, *Helsinki University of Technology, Finland*
Gavin Lowe, *Oxford University, UK*
Teresa Lunt, *Palo Alto Research Center, USA*

**Program Committee (continued):**

Phil MacKenzie, *Bell Labs - Lucent Technologies, USA*
Hiroshi Maruyama, *IBM Research Tokyo, Japan*
Ludovic Mé, *Supélec, France*
Catherine Meadows, *Naval Research Laboratory, USA*
John Mitchell, *Stanford University, USA*
Andrew Myers, *Cornell University, USA*
Chanathip Namprempre, *Thammasat University, Thailand*
Pekka Nikander, *Ericsson Research, Finland*
Tatsuaki Okamoto, *NTT Research, Japan*
Vern Paxson, *ICSI / LBNL, USA*
Adrian Perrig, *Carnegie Mellon University, USA*
David Pointcheval, *CNRS-ENS, France*
Joachim Posegga, *SAP and University of Hamburg, Germany*
Josyula R. Rao, *IBM Research, USA*
Indrakshi Ray, *Colorado State University, USA*
Juha Röning, *University of Oulu, Finland*
Michael Rusinowitch, *INRIA Lorraine, France*
Rei Safavi-Naini, *University of Wollongong, Australia*
Tomas Sander, *Hewlett-Packard, USA*
Andre Scedrov, *University of Pennsylvania, USA*
Steve Schneider, *University of Surrey, UK*
Matthias Schunter, *IBM Zurich Research Lab, Switzerland*
Jonathan Shapiro, *Johns Hopkins University, USA*
Morris Sloman, *Imperial College London, UK*
Dawn Song, *Carnegie Mellon University, USA*
Gene Tsudik, *University of California Irvine, USA*
Els Van Herreweghen, *IBM Zurich Research Lab, Switzerland*
Serge Vaudenay, *EPFL Lausanne, Switzerland*
Dennis Volpano, *Cranite Systems Inc., USA*
Dan S. Wallach, *Rice University, USA*

**Sponsor:**

**with contributions from:**

# External Reviewers

Adam Smith
Adriano Peron
Aki Helin
Alessandro Provetti
Alexander Pretschner
Alexandru Baltag
Alvaro Cardenas
Andreas Wespi
Andrei Serjantov
Andrew Martin
Anna Corazza
Anna Lysyanskaja
Anna Squicciarini
Arun Hampapur
Axel Tanner
Barry Mulcahy
Ben Aziz
Benjamin Morin
Bernard Vivinis
Bidan Christophe
Broemme Arslan
Carlo Blundo
Carlos Caleiro
Chris Vanden Berghe
Christian Wieser
Christopher Giblin
Claude Castelluccia
Clemente Galdi
Cristina Buchholz
Cristina Nita-Rotaru
Cynthia Kuo
Dae-Kyoo Kim
Daisuke Takuma
Dario Catalano
Darko Kirovski
Debanjan Saha
Debin Gao
Diana Senn
Diego Zamboni
Dogan Kesdogan
Don Coppersmith
Duong Hieu Phan
Dusko Pavlovic
Einar Mykletun
Eric Totel
Fabien Pouget
Florian Probst
Gelareh Taban
Gerhard Hancke
Gildas Avoine
Gordon Rohrmair
Greg Bronevetsky
Günter Karjoth
Heejo Lee
Heiko Mantel
Henrich C. Poehls
Heye Laurent
Hiroaki Etoh
Hongbin Zhou
Huaxiong Wang
Iliano Cervesato
Ilya Mironov
Indrajit Ray
Jacques Fournier
James Newsome
James Riordan
Jan Seedorf
Jarkko Lämsä
Jean Monnerat
Jeong Yi
Jessica Staddon
Ji-Won Byun
Jiangtao Li
Joachim Wide
Jonathan Moffett
Joonsang Baek
Josyula R. Rao
Jouga Bernard
Jouni Viinikka
Jürgen Doser
Julien Brouchier
Klaus Julisch
Klaus Plößl
Kostas Anagnostakis
Lantian Zheng
Laurent Vigneron
Lea Kissner
Leonid Reyzin
Lexi Pimenidis
Louis Granboulan
Lujo Bauer
Mahesh Tripunitara
Maithili Narasimha
Margus Freudenthal
Maria L. Damiani
Marko Laakso
Martin Hirt
Maryann Hondo
Masayuki Numao
Mathieu Baudet
Mats Näslund
Meelis Roos
Megumi Nakamura
Mella Giovanni
Michael Backes
Michael Collins
Michael Goldsmith
Michael Huth
Michael May
Michael Naef
Michael Steiner
Michael Waidner
Michel Abdalla
Michiharu Kudoh
Mike Marr
Mohamed Shehab
Morton Swimmer
Naranker Dulay
Nate Nystrom
Nedeljko Cvejic
Neil Evans
Niels Ferguson
Nitesh Saxena
Olga Kouchnarenko
Pascal Junod
Pasi Eronen
Pau-chen Cheng
Paul Hankes Drielsma
Paul Syverson
Peer Wichmann
Pekka Pietikäinen
Philippe Golle
Philippe Oechslin
Pierre-Alain Fouque
Pierre-Cyrille
Pino Persiano
Radu State
Ran Canetti
Ravi Pandya
Reza Curtmola
Riccardo Pucella
Roberto Delicata
Roger Kilian-Kehr
Rosario Gennaro
Ruchika Agarwal
Satoshi Hada
Satu Schaefer
Sebastian Mödersheim
Seiji Munetoh
Sherif Yusuf
Shobha Venkataraman
Stanislaw Jarecki
Stefan Wolf
Stephen Chong
Stephen Lewis
Steven Murdoch
Suresh Chari
Sven Laur
Swaroop Sridhar
Tadek Pietraszek
Tal Rabin
Tarek Abbes
Ted Wobber
Theodore Hong
Thomas Baignères
Thomas Holenstein
Thomas Nowey
Thomas Quillinan
Tim Ebringer
Timo Hyart
Ting Yu
Tobias Kölsch
Tomi Nylund
Vaibhav Gowadia
Veronique Cortier
Willy Susilo
Xuhua Ding
Yi Lu
Yi Mu
Ziad Bizri