



CS 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



with contributions from

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

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



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



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**

Copyright © 2004 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: 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 Pfizmann, 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 Paxson (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 administrative 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

| | |
|---|------|
| CCS 2004 Conference Organization | viii |
|---|------|

| | |
|----------------------|------|
| Sponsor | viii |
|----------------------|------|

Session 1: Keynote speech

| | |
|--|---|
| • Trusting a Trusted System | 1 |
| J. McLean (<i>Naval Research Laboratory</i>) | |

Session 2: Network Intrusions

| | |
|---|----|
| • Operational Experiences with High-Volume Network Intrusion Detection | 2 |
| H. Dreger, A. Feldmann (<i>TU München</i>), V. Paxson (<i>ICSI/LBNL</i>), R. Sommer (<i>TU München</i>) | |
| • On the Difficulty of Scalably Detecting Network Attacks | 12 |
| K. Levchenko, R. Paturi, G. Varghese (<i>University of California at San Diego</i>) | |
| • Testing Network-based Intrusion Detection Signatures Using Mutant Exploits | 21 |
| G. Vigna, W. Robertson, D. Balzarotti (<i>University of California at Santa Barbara</i>) | |
| • Payload Attribution via Hierarchical Bloom Filters | 31 |
| K. Shanmugasundaram, H. Brönnimann, N. Memon (<i>Polytechnic University</i>) | |

Session 3: Access control

| | |
|--|----|
| • On Mutually-Exclusive Roles and Separation of Duty | 42 |
| N. Li, Z. Bizri, M. V. Tripunitara (<i>Purdue University</i>) | |
| • KNOW Why Your Access Was Denied: Regulating Feedback for Usable Security | 52 |
| A. Kapadia, G. Sampemane, R. H. Campbell (<i>University of Illinois at Urbana-Champaign</i>) | |
| • Comparing the Expressive Power of Access Control Models | 62 |
| M. V. Tripunitara, N. Li (<i>Purdue University</i>) | |

Session 4: Applied cryptography

| | |
|---|----|
| • Attacking and Repairing the WinZip Encryption Scheme | 72 |
| T. Kohno (<i>University of California at San Diego</i>) | |
| • Reusable Cryptographic Fuzzy Extractors | 82 |
| X. Boyen (<i>Voltage Security</i>) | |
| • Cryptanalysis of a Provably Secure CRT-RSA Algorithm | 92 |
| D. Wagner (<i>University of California at Berkeley</i>) | |

Session 5: Network security

| | |
|--|-----|
| • Pong-Cache Poisoning in GUESS | 98 |
| N. Daswani, H. Garcia-Molina (<i>Stanford University</i>) | |
| • Web Tap: Detecting Covert Web Traffic | 110 |
| K. Borders, A. Prakash (<i>University of Michigan</i>) | |
| • On Achieving Software Diversity for Improved Network Security using Distributed Coloring Algorithms | 121 |
| A. J. O'Donnell, H. Sethu (<i>Drexel University</i>) | |

Session 6: Credentials

| | |
|--|-----|
| • Direct Anonymous Attestation | 132 |
| E. Brickell (<i>Intel Corporation</i>), J. Camenisch (<i>IBM Research</i>), L. Chen (<i>HP Laboratories</i>) | |

| | |
|---|-----|
| • Concealing Complex Policies with Hidden Credentials | 146 |
| R. W. Bradshaw, J. E. Holt, K. E. Seamons (<i>Brigham Young University</i>) | |
| • k-Anonymous Secret Handshakes with Reusable Credentials | 158 |
| S. Xu (<i>University of Texas at San Antonio</i>), M. Yung (<i>Columbia University</i>) | |
| • Group Signatures with Verifier-Local Revocation | 168 |
| D. Boneh, H. Shacham (<i>Stanford University</i>) | |

Session 7: Information flow

| | |
|---|-----|
| • IP Covert Timing Channels: Design and Detection | 178 |
| S. Cabuk (<i>Purdue University</i>), C. E. Brodley (<i>Tufts University</i>), C. Shields (<i>Georgetown University</i>) | |
| • Private Inference Control (Extended Abstract) | 188 |
| D. Woodruff (<i>Massachusetts Institute of Technology</i>), J. Staddon (<i>Palo Alto Research Center</i>) | |
| • Security Policies for Downgrading | 198 |
| S. Chong, A. C. Myers (<i>Cornell University</i>) | |

Session 8: Privacy

| | |
|--|-----|
| • Privacy and Security in Library RFID Issues, Practices, and Architectures | 210 |
| D. Molnar, D. Wagner (<i>University of Berkeley</i>) | |
| • Parallel Mixing | 220 |
| P. Golle (<i>Palo Alto Research Center</i>), A. Juels (<i>RSA Laboratories</i>) | |
| • Fragile Mixing | 227 |
| M. K. Reiter (<i>Carnegie Mellon University</i>), X. Wang (<i>Indiana University at Bloomington</i>) | |

Session 9: Puzzles and users

| | |
|---|-----|
| • A PIN-Entry Method Resilient Against Shoulder Surfing | 236 |
| V. Roth (<i>OGM Laboratory LLC</i>), K. Richter (<i>ZGDV</i>), R. Freidinger (<i>Technical University Darmstadt</i>) | |
| • New Client Puzzle Outsourcing Techniques for DoS Resistance | 246 |
| B. Waters (<i>Princeton University</i>), A. Juels (<i>RSA Laboratories</i>), J. A. Halderman, E. W. Felten (<i>Princeton University</i>) | |
| • Mitigating Bandwidth-Exhaustion Attacks using Congestion Puzzles | 257 |
| X.F. Wang (<i>Indiana University at Bloomington</i>), M. K. Reiter (<i>Carnegie Mellon University</i>) | |

Session 10: Applications of formal methods

| | |
|--|-----|
| • Verifying Policy-Based Security for Web Services | 268 |
| K. Bhargavan, C. Fournet, A. D. Gordon (<i>Microsoft Research</i>) | |
| • A Decision Procedure for the Verification of Security Protocols with Explicit Destructors (Extended Abstract) | 278 |
| S. Delaune (<i>France Télécom R&D</i>), F. Jacquemard (<i>INRIA</i>) | |
| • Using Build-Integrated Static Checking to Preserve Correctness Invariants | 288 |
| H. Chen (<i>University of California at Berkeley</i>), J. S. Shapiro (<i>Johns Hopkins University</i>) | |

Session 11: Operating systems security

| | |
|--|-----|
| • On the Effectiveness of Address-Space Randomization | 298 |
| H. Shacham, M. Page, B. Pfaff, E.-J. Goh, N. Modadugu, D. Boneh (<i>Stanford University</i>) | |
| • Attestation-based Policy Enforcement for Remote Access | 308 |
| R. Sailer, T. Jaeger, X. Zhang, L. van Doorn (<i>IBM T.J. Watson Research Center</i>) | |
| • Gray-Box Extraction of Execution Graphs for Anomaly Detection | 318 |
| D. Gao, M. K. Reiter, D. Song (<i>Carnegie Mellon University</i>) | |

Session 12: Cryptographic tools

| | |
|---|-----|
| • The Dual Receiver Cryptosystem and Its Applications | 330 |
| T. Diament, H. K. Lee, A. D. Keromytis, M. Yung (<i>Columbia University</i>) | |
| • Versatile Padding Schemes for Joint Signature and Encryption | 344 |
| Y. Dodis, M. J. Freedman (<i>New York University</i>), S. Jarecki (<i>University of California at Irvine</i>), S. Walfish (<i>New York University</i>) | |
| • ID-Based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption | 354 |
| D. Yao (<i>Brown University</i>), N. Fazio, Y. Dodis (<i>New York University</i>), A. Lysyanskaya (<i>Brown University</i>) | |
| Author Index | 364 |

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 Fitz, *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 Rönning, *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:



**U.S. Army
Research Office**

External Reviewers

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