

CCS'05

**Proceedings of the
12th ACM Conference on Computer
and Communications Security**

**November 7-11, 2005
Alexandria, Virginia, USA**



Catherine Meadows & Paul Syverson, *Editors*

**Sponsored by
ACM Special Interest Group on Security, Audit and Control (SIGSAC)**

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

Copyright © 2005 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: 1-59593-226-7

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 459050
Printed in the USA

Welcome to CCS 2005

It is a pleasure and honor to welcome you to the 12th 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, eight workshops and four tutorials that cover a variety of interests and disciplines in the area of computer and communications security.

Many individuals have contributed to the success of this conference. First, I would like to thank Catherine Meadows, 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 38/250. Second, I would like to thank the industry track chair, Ari Juels and the members of the industry program committee for putting together a fantastic program.

I would like to extend my appreciation to Pierangela Samarati, 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: Rei Safavi-Naini (Workshop on Digital Rights Management); Peng Ning and Wenliang Du (Workshop on Security of Ad Hoc and Sensor Networks); Sabrina De Capitani di Vimercati and Roger Dingledine (Workshop on Privacy in Electronic Society); Angelos D. Keromytis (Workshop on Rapid Malcode); Ralf Kusters and John Mitchell (Workshop on Formal Methods in Security Engineering: From Specifications to Code); Ernesto Damiani and Hiroshi Maruyama (Workshop on Secure Web Services); Atsuhiko Goto (Workshop on Digital Identity Management); and Bill Yurcik (Workshop on Workshop on Storage Security and Survivability). While the last two workshops are new, the first 6 of the 8 workshops were held in earlier years in conjunction with CCS. Next, I would like to express my thanks to Rebecca Wright for having excellent tutorials in this year's program. The program includes four tutorials offered in parallel with the research paper sessions.

I am grateful to Douglas Maughan for agreeing to deliver the Conference keynote address, Peng Ning for managing the budget, Paul Syverson 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 wish to express my appreciation to the CCS steering committee, Sushil Jajodia (Chair) Ravi Ganesan, Ravi Sandhu, and Pierangela Samarati, for their continued support. I would also like to acknowledge the administrative staff of the ACM SIGSAC and George Mason University for their support, and Executive Events for helping with the registrations.

I wish to thank the following institutions for their generous financial support: Defense Advanced Research Projects Agency, The Army Research Office, IBM Research, Microsoft 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

Message From the Program Chair

I am delighted to join Vijay Atluri in welcoming you to the *12th ACM Conference on Computer and Communications Security*. These proceedings contain papers presented at the research track, and abstracts of invited talks presented in the industry track.

A total of 250 papers were submitted to the research track this year. These were reviewed by a committee of 41 experts. Each paper was assigned to three program committee members. Papers were anonymized, so that reviewers could not identify the author of a paper. Program committee members could use outside reviewers, but were responsible for the contents of the review, and for defending it during discussion of the paper.

The reviewing phase was followed by a three week long phase of intense discussion, in which the opinion of outside experts was often solicited as well. Every paper for which at least one reviewer recommended acceptance was discussed until a consensus was reached. A total of 38 papers were selected for publication and presentation. This 15% acceptance rate maintains CCS's standing as one of the most selective conferences in information security.

I am grateful to the members of the program committee, whose hard work and effort made it possible to put this program together. The committee was smaller than in previous years, which meant more work for individual members, but I also think that it helped in providing a cohesive group that participated actively in the online discussions.

I would like to thank the members of the steering committee, Sushil Jajodia, Ravi Sandhu, Ravi Ganesan, and Pierangela Samarati, for their support, especially in authorizing the funding for the use of the START conference system, which greatly simplified the running of the conference. I would also like to thank the program chairs from the last two years, Birgit Pfizmann and Vijay Atluri, for their support and advice, and our sponsors, the Army Research Office, DARPA, IBM Research, Microsoft Research, and DoCoMo Communication Laboratories, for their generous financial support. Finally, I'd like to thank Gail-Joon Ahn and Paul Syverson, the publicity chair and the proceedings chair, for their hard work in publicizing the conference and putting the proceedings together, thus freeing me for the task of assembling the program.

I'd like to finish by thanking all the authors who submitted their papers to CCS. Whether or not your paper was accepted, you have helped contribute to the success of CCS, and we appreciate your hard work.

We all hope that you enjoy the program. We are looking forward to your participation in the conference, and expect it to be as dynamic and stimulating as it has been in past years.

Catherine Meadows
Research Track Program Chair

Table of Contents

CCS 2005 Conference Organization	viii
Sponsor & Supporters	ix
External Reviewers	x

Keynote Address

Chair: C. Meadows (*Naval Research Laboratory*)

- **Homeland Security: Cyber Security R&D Initiatives** 1
D. Maughan (*Department of Homeland Security*)

Session 1: Formal Analysis of Crypto Protocols

Chair: A. Scedrov (*University of Pennsylvania*)

- **A Modular Correctness Proof of IEEE 802.11i and TLS** 2
C. He, M. Sundararajan, A. Datta, A. Derek, J. C. Mitchell (*Stanford University*)
- **Deciding Security of Protocols against Off-line Guessing Attacks** 16
M. Baudet (*LSV – CNRS & INRIA Futurs Project SECSI & ENS Cachan*)
- **Secrecy Types for a Simulatable Cryptographic Library** 26
P. Laud (*Tartu University*)

Session 2: Trust Management

Chair: M. Winslett (*University of Illinois*)

- **Preventing Attribute Information Leakage in Automated Trust Negotiation** 36
K. Irwin, T. Yu (*North Carolina State University*)
- **Automated Trust Negotiation Using Cryptographic Credentials** 46
J. Li, N. Li (*Purdue University*), W. H. Winsborough (*University of Texas at San Antonio*)
- **Secure Collaboration in Mediator-Free Environments** 58
M. Shehab, E. Bertino, A. Ghafoor (*Purdue University*)

Session 3: Privacy and Anonymity

Chair: R. Wright (*Stevens Institute of Technology*)

- **Applications of Secure Electronic Voting to Automated Privacy-Preserving Troubleshooting** 68
Q. Huang (*Princeton University*), D. Jao, H. J. Wang (*Microsoft Research*)
- **Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet** 81
X. Wang, S. Chen, S. Jajodia (*George Mason University*)
- **Untraceable RFID Tags via Insubvertible Encryption** 92
G. Ateniese (*The Johns Hopkins University*), J. Camenisch (*IBM Research*),
B. de Medeiros (*Florida State University*)
- **Obfuscated Databases and Group Privacy** 102
A. Narayanan, V. Shmatikov (*The University of Texas at Austin*)

Session 4: Authentication

Chair: J. Katz (*University of Maryland*)

- **New Approaches for Deniable Authentication** 112
M. Di Raimondo (*Università di Catania*), R. Gennaro (*IBM T.J. Watson Research Center*)

- **On Authenticated Computing and RSA-based Authentication** 122
J.-P. Seifert (*Intel Corporation*)
- **Aggregated Path Authentication for Efficient BGP Security** 128
M. Zhao, S. W. Smith (*Dartmouth College*), D. M. Nicol (*University of Illinois at Urbana-Champaign*)
- **Improving Brumley and Boneh Timing Attack on Unprotected SSL Implementations** 139
O. Aciicmez (*Oregon State University*), W. Schindler (*Bundesamt für Sicherheit in der Informationstechnik*),
Ç. K. Koç (*Oregon State University*)

Session 5: Access Control

Chair: P. Syverson (*Naval Research Laboratory*)

- **CPOL: High-Performance Policy Evaluation** 147
K. Borders, X. Zhao, A. Prakash (*University of Michigan*)
- **Understanding and Developing Role-Based Administrative Models** 158
J. Crampton (*University of London*)
- **PeerAccess: A Logic for Distributed Authorization** 168
M. Winslett, C. C. Zhang (*University of Illinois at Urbana-Champaign*), P. A. Bonatti (*Università di Napoli*)

Session 6: Key Management, Key Exchange, & Pseudo-Random Generation

Chair: J. Feigenbaum (*Yale University*)

- **Modeling Insider Attacks on Group Key-Exchange Protocols** 180
J. Katz, J. S. Shin (*University of Maryland*)
- **Dynamic and Efficient Key Management for Access Hierarchies** 190
M. J. Atallah, K. B. Frikken, M. Blanton (*Purdue University*)
- **A Model and Architecture for Pseudo-Random Generation and Applications to `/dev/random`** 203
B. Barak (*Princeton University*), S. Halevi (*IBM T.J. Watson Research Center*)

Session 7: Intrusion Detection and Prevention

Chair: S. Jha (*University of Wisconsin*)

- **Fast and Automated Generation of Attack Signatures: A Basis for Building Self-Protecting Servers** 213
Z. Liang, R. Sekar (*Stony Brook University*)
- **Automatic Diagnosis and Response to Memory Corruption Vulnerabilities** 223
J. Xu, P. Ning, C. Kil, Y. Zhai, C. Bookholt (*North Carolina State University*)
- **On Deriving Unknown Vulnerabilities from Zero-Day Polymorphic and Metamorphic Worm Exploits** 235
J. R. Crandall, Z. Su, S. F. Wu (*University of California at Davis*),
F. T. Chong (*University of California at Santa Barbara*)
- **Countering DoS Attacks With Stateless Multipath Overlays** 249
A. Stavrou, A. D. Keromytis (*Columbia University*)

Session 8: Security for Diffuse Computing

Chair: J. Guttman (*MITRE*)

- **A Framework for Concrete Reputation-Systems with Applications to History-Based Access Control** 260
K. Krukow, M. Nielsen (*University of Aarhus*), V. Sassone (*University of Sussex*)
- **An Auctioning Reputation System Based on Anomaly Detection** 270
S. Rubin, M. Christodorescu, V. Ganapathy, J. T. Giffin, L. Kruger, H. Wang (*University of Wisconsin*)

- **On the Cost-Ineffectiveness of Redundancy in Commercial P2P Computing** 280
M. Yurkewych, B. N. Levine, A. L. Rosenberg (*University of Massachusetts*)
- **Securing Publish-Subscribe Overlay Services with EventGuard** 289
M. Srivatsa, L. Liu (*Georgia Institute of Technology*)

Session 9: Cryptography

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

- **Password Authenticated Key Exchange Using Hidden Smooth Subgroups** 299
C. Gentry, P. Mackenzie, Z. Ramzan (*DoCoMo USA Laboratories*)
- **Proxy Re-Signatures: New Definitions, Algorithms, and Applications** 310
G. Ateniese (*The Johns Hopkins University*), S. Hohenberger (*Massachusetts Institute of Technology*)
- **Direct Chosen Ciphertext Security from Identity-Based Techniques** 320
X. Boyen (*Voltage Inc.*), Q. Mei (*Southwest Jiaotong University*), B. Waters (*Stanford University*)

Session 10: Automated Analysis

Chair: N. Li (*Purdue University*)

- **Automatic Placement of Authorization Hooks in the Linux Security Modules Framework** 330
V. Ganapathy (*University of Wisconsin*), T. Jaeger (*Pennsylvania State University*), S. Jha (*University of Wisconsin*)
- **Control-Flow Integrity: Principles, Implementations, and Applications** 340
M. Abadi (*University of California at Santa Cruz*), M. Budiu, Ú. Erlingsson (*Microsoft Research*), J. Ligatti (*Princeton University*)
- **Preventing Format-String Attacks via Automatic and Efficient Dynamic Checking** 354
M. F. Ringenburt, D. Grossman (*University of Washington*)

Session 11: Attacking Passwords and Bringing Down The Network

Chair: C. Meadows (*Naval Research Laboratory*)

- **Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff** 364
A. Narayanan, V. Shmatikov (*The University of Texas at Austin*)
- **Keyboard Acoustic Emanations Revisited** 373
L. Zhuang, F. Zhou, J. D. Tygar (*University of California at Berkeley*)
- **Misbehaving TCP Receivers Can Cause Internet-Wide Congestion Collapse** 383
R. Sherwood, B. Bhattacharjee (*University of Maryland*), R. Braud (*University of California at San Diego*)
- **Exploiting Open Functionality in SMS-Capable Cellular Networks** 393
W. Enck, P. Traynor, P. McDaniel, T. La Porta (*The Pennsylvania State University*)

Industry Track Invited Talks

- **Security Market: Incentives for Disclosure of Vulnerabilities** 405
P. P. Swire (*Ohio State University*)
- **Identity-Based Encryption From Algorithm to Enterprise Deployment** 406
G. Appenzeller (*Voltage Security*)
- **Biometrics Hit the Mainstream: An Analysis of Security and Privacy Implications** 407
V. Bjorn (*DigitalPersona*)

Author Index 408

CCS 2005 Conference Organization

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

Program Chair (Research Track): Catherine Meadows, *Naval Research Laboratory, USA*

Program Chair (Industry Track): Ari Juels, *RSA Laboratories, USA*

Proceedings Chair: Paul Syverson, *Naval Research Laboratory, USA*

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

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

Tutorials Chair: Rebecca Wright, *Stevens Institute of Technology, USA*

Workshops Chair: Pierangela Samarati, *University of Milan, Italy*

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

Program Committee: David Basin, *ETH Zurich, Switzerland*
Dan Boneh, *Stanford University, USA*
Jan Camenisch, *IBM Research, Switzerland*
Pierpaolo Degano, *University of Pisa, Italy*
George Dinolt, *Naval Postgraduate School, USA*
Yevgeniy Dodis, *New York University, USA*
Joan Feigenbaum, *Yale University, USA*
Stephanie Forrest, *University of New Mexico, USA*
Cédric Fournet, *Microsoft Research, UK*
Dieter Gollmann, *Hamburg University of Technology, Germany*
Roberto Gorrieri, *University of Bologna, Italy*
Joshua Guttman *MITRE, USA*
Cynthia Irvine, *Naval Postgraduate School, USA*
Somesh Jha, *University of Wisconsin, USA*
Jonathan Katz, *University of Maryland, USA*
Angelos Keromytis, *Columbia University, USA*
Carl Landwehr, *University of Maryland, USA*
Peeter Laud, *University of Tartu, Estonia*
Ninghui Li, *Purdue University, USA*
Javier Lopez, *University of Malaga, Spain*
Hiroshi Maruyama, *IBM Japan, Japan*
John Mitchell, *Stanford University, USA*
George Mohay, *Queensland University of Technology, Australia*
Mats Näslund, *Ericsson Research, Sweden*

Program Committee (continued): Eiji Okamoto, *University of Tsukuba, Japan*
Hilarie Orman, *Purple Streak, USA*
Radia Perlman, *Sun Microsystems, USA*
Adrian Perrig, *Carnegie Mellon University, USA*
Radha Poovendran, *University of Washington, USA*
Rei Safavi-Naini, *University of Wollongong, Australia*
Andre Scedrov, *University of Pennsylvania, USA*
Kang Shin, *University of Michigan, USA*
Vitaly Shmatikov, *University of Texas, USA*
Dawn Song, *Carnegie-Mellon University, USA*
Giovanni Vigna, *UC Santa Barbara, USA*
David Wagner, *UC Berkeley, USA*
Dan Wallach, *Rice University, USA*
Andreas Westfeld, *TU Dresden, Germany*
Marianne Winslett, *University of Illinois, USA*
Rebecca Wright, *Stevens Institute of Technology, USA*
Lenore Zuck, *University of Illinois at Chicago, USA*

Sponsor:



with contributions from:



IBM Research



**U.S. Army
Research Office**

External Reviewers

Martin Abadi	Gianluca Dini	Roberto Lucchi	R. Sekar
Isaac Agudo	Juergen Doser	Andrea Maggiolo-	Arvind Seshadri
Marco Aldinucci	Carl Ellison	Schettini	Hovav Shacham
Kostas Anagnostakis	Fernando Esponda	Ajay Mahimkar	Nicholas Sheppard
Anne Anderson	Nelly Fazio	Vittorio Maniezzo	Elaine Shi
Stig Andersson	Gerardo Fernandez	Jonathan McCune	Rishi Rakesh Sinha
Tuomas Aura	GianLuigi Ferrari	John McDermott	Robert H. Sloan
Joonsang Baek	Elke Franz	Hernan Melgratti	Diana Smetters
Justin Balthrop	Vinod Ganapathy	Nicola Mezzetti	Jon A. Solworth
Amnon Barak	Debin Gao	Takuya Mishina	Dieter Sommer
Paul Barford	Ryan Gerety	David Molnar	Angelos Stavrou
Matthew Barrick	Vittorio Ghini	Carlo Montangero	Sandra Steinbrecher
Massimo Bartoletti	Jonathon Giffin	Jose A. Montenegro	Salvatore J. Stolfo
Steve Bellovin	Andy Gordon	Alberto Montresor	Michael Szydlowski
Vicente Benjumea	Claudio Guidi	Ruggero Morselli	Gelareh Taban
Mike Bergmann	Min Gyuang	Seiji Munetoh	Patrick Tague
Abhilasha Bhargav	Satoshi Hada	Darren Mutz	Anat Talmy
Karthik Bhargavan	Ragib Hasan	Megumi Nakamura	Axel Tanner
Richard Black	Yunxiao He	Arvind Narayanan	Dongvu Tonien
Bruno Blanchet	Manuel Hilty	James Newsome	Mahesh V. Tripunitara
Rolf Blom	Steven Hofmeyr	Antonio Nicolosi	Angelo Troina
Chiara Bodei	Susan Hohenberger	Lars Olson	Eran Tromer
Marine Boden	Jeffery Horton	Jose A. Onieva	Stephen Tse
Rainer Böhme	Kenneth Ingham	Bryan Parno	Emilio Tuosto
Luciano Bononi	John Ioannidis	Christopher Peikert	Fredrik Valeur
Abhijit Bose	Sotiris Ioannidis	Marinella Petrocchi	Chris Vanden Berghe
Carl Bosley	Stanislaw Jarecki	Carla Piazza	V.N. Venkatakrishnan
Xavier Boyen	Sundararaman Jeyaraman	David Pointcheval	Shobha Venkataraman
Andrea Bracciali	Mattias Johansson	Makan Pourzandi	Luca Viganò
Chiara Braghin	Myong Kang	Alexander Pretschner	Shabsi Walfish
Justin Brickell	Josh Karlin	Bartosz Przydatek	Hao Wang
Achim Brucker	Jintae Kim	Prashant Puniya	Lihua Wang
David Brumley	Lea Kissner	Paola Quaglia	Christina Warrender
Hal Burch	Boris Koepf	James Riordan	Yuji Watanabe
Matthew Burnside	Stefan Köpsell	Nilo Rivera	Matthew Williamson
Bill Bush	Thomas Kriegelstein	William Robertson	Abraham Yaar
Ji-Won Byun	Karl Krukow	Michael Roe	Mariem I. Yague
Alvaro Cardenas	Michiharu Kudo	Rodrigo Roman	Aleksandr Yampolskiy
Haowen Chan	Cynthia Kuo	Meelis Roos	Jisoo Yang
Min-gyu Cho	Loukas Lazos	Shai Rubin	Sachiko Yoshihama
Mihai Christodorescu	Adam Lee	Javier Salido	Lan Yu
Andrew Clark	Wenke Lee	Vladimiro Sassone	Gianluigi Zavattaro
Sebastian Clauß	Tim Levin	Hada Satoshi	Charles Zhang
Michael Collins	Jiangtao Li	Bradley Schatz	Sheng Zhong
Weidong Cui	Mingyan Li	Steve Schneider	Jacob Zimmermann
Debabrata Dash	Helger Lipmaa	Antje Schneidewind	Roberto Zunino
Renzo Davoli	Michael Locasto	Richard Schroepel	