

**Proceedings of the
9th ACM Conference
on
Computer and Communications Security**



2 0 0 2

**Washington, DC, USA
November 18-22, 2002**

Edited by: Vijay Atluri

**Sponsored by:
ACM SIGSAC**



Table of Contents

Conference Committee	vii
Contributions	vii
Program Committee	vii-viii
External Reviewers	viii
 Session: Cryptographic Protocols	
• Authenticated Encryption in SSH: Provably Fixing the SSH Binary Packet Protocol	1
Mihir Bellare, Tadayoshi Kohno (<i>Univ. of California at San Diego</i>), Chanathip Namprempre (<i>Thammasat Univ. Thailand</i>)	
• The Verification of an Industrial Payment Protocol: The SET Purchase Phase	12
Giampaolo Bella (<i>University of Cambridge</i>), Fabio Massacci (<i>Università di Trento</i>), Lawrence C. Paulson (<i>University of Cambridge</i>)	
• Design and Implementation of the Idemix Anonymous Credential System	21
Jan Camenisch, Els Van Herreweghen (<i>Zurich Research Laboratory</i>)	
 Session: Key Management and Key Exchange	
• A Temporal Key Management Scheme for Secure Broadcasting of XML Documents	31
Elisa Bertino, Barbara Carminati (<i>DSI Università di Milano</i>), Elena Ferrari (<i>DCFM Università dell'Insubria</i>)	
• A Key-Management Scheme for Distributed Sensor Networks	41
Laurent Eschenauer, Virgil D. Gligor (<i>University of Maryland</i>)	
• Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols	48
William Aiello, Steven M. Bellovin, Matt Blaze (<i>AT&T Labs Research</i>), Ran Canetti (<i>IBM T.J. Watson Research Center</i>), John Ioannidis (<i>AT&T Labs Research</i>), Angelos D. Keromytis (<i>Columbia University</i>), Omer Reingold (<i>AT&T Labs Research</i>)	
 Session: Emerging Applications	
• Defending Against Redirect Attacks in Mobile IP	59
Robert H. Deng, Jianying Zhou, Feng Bao (<i>Labs for Information Technology</i>)	
• Almost Entirely Correct Mixing With Applications to Voting	68
Dan Boneh, Philippe Golle (<i>Stanford University</i>)	
• DRM: Doesn't Really Mean Digital Copyright Management	78
L Jean Camp (<i>Kennedy School Of Government</i>)	
 Session: Cryptography	
• Asynchronous Verifiable Secret Sharing and Proactive Cryptosystems	88
Christian Cachin, Klaus Kursawe, Anna Lysyanskaya, Reto Stroh (<i>Zurich Research Laboratory</i>)	
• Authenticated-Encryption with Associated-Data	98
Phillip Rogaway (<i>University of California at Davis</i>)	
• Generic Implementations of Elliptic Curve Cryptography using Partial Reduction	108
Nils Gura, Hans Eberle, Sheueling Chang Shantz (<i>Sun Microsystems</i>)	

Session: Network Security

- **Efficient Packet Marking for Large-Scale IP Traceback** 117
Michael T. Goodrich (*University of California at Irvine*)
- **Sensor-Based Intrusion Detection for Intra-Domain Distance-Vector Routing** 127
Vishal Mittal, Giovanni Vigna (*University of California at Santa Barbara*)
- **Code Red Worm Propagation Modeling and Analysis** 138
Cliff Changchun Zou, Weibo Gong, Don Towsley (*University of Massachusetts*)

Session: Authentication and Authorization

- **Silicon Physical Random Functions** 148
Blaise Gassend, Dwaine Clarke, Marten van Dijk, Srinivas Devadas (*Massachusetts Institute of Technology*)
- **Securing Passwords Against Dictionary Attacks** 161
Benny Pinkas (*HP Labs, Rutgers University*), Tomas Sander (*HP Labs*)
- **Policy Algebras for Access Control — The Predicate Case** 171
Duminda Wijesekera, Sushil Jajodia (*George Mason University*)

Session: Peer to Peer Networks

- **Query-Flood DoS Attacks in Gnutella** 181
Neil Daswani, Hector Garcia-Molina (*Stanford University*)
- **Tarzan: A Peer-to-Peer Anonymizing Network Layer** 193
Michael J. Freedman (*NYU*), Robert Morris (*MIT Lab for Computer Science*)
- **A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks** 207
Ernesto Damiani (*DTI-Università di Milano*), Sabrina De Capitani di Vimercati (*DEA-Università di Brescia*), Stefano Paraboschi (*DEI-Politecnico di Milano*), Pierangela Samarati (*DTI-Università di Milano*), Fabio Violante (*DEI-Politecnico di Milano*)

Session: Analysis and Verification

- **Scalable, Graph-Based Network Vulnerability Analysis** 217
Paul Ammann, Duminda Wijesekera, Saket Kaushik (*George Mason University*)
- **Runtime Verification of Authorization Hook Placement for the Linux Security Modules Framework** 225
Antony Edwards, Trent Jaeger, Xiaolan Zhang (*IBM T.J. Watson Research Center*)
- **MOPS: an Infrastructure for Examining Security Properties of Software** 235
Hao Chen, David Wagner (*University of California at Berkeley*)

Session: Intrusion Detection

- **Constructing Attack Scenarios through Correlation of Intrusion Alerts** 245
Peng Ning, Yun Cui, Douglas S. Reeves (*NC State University*)
- **Mimicry Attacks on Host-Based Intrusion Detection Systems** 255
David Wagner, Paolo Soto (*University of California at Berkeley*)
- **Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions** 265
R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, S. Zhou (*Stony Brook University*)

- **Author Index** 275