Table of Contents

Message from General Chair.....iii
Message from the Program Chair.....iv
Conference Committee..... v

Session 1: Group Key Management

Communication Complexity of Group Key Distribution.....1
Klaus Becker (τ^3 Security Engineering, Switzerland)
Uta Wille (IBM Zurich Research Laboratory, Switzerland)

Key Management for Encrypted Broadcast.....7
Avishai Wool (Bell Laboratories-Lucent Technologies, USA)

Authenticated Group Key Agreement and Friends.....17
Giuseppe Ateniese (USC Information Sciences Institute, USA)
Michael Steiner (IBM Zurich Research Laboratory, Switzerland)
Gene Tsudik (USC Information Sciences Institute, USA)

Session 2: Anonymity

The Design, Implementation and Operation of an Email Pseudonym Server.....27
David Mazières and M. Frans Kaashoek (MIT Laboratory for Computer Science, USA)

Panel: Anonymity on the Internet.....37
Paul Syverson, (Naval Research Laboratory, USA)

Session 3: Mobile Code Security

History-Based Access Control for Mobile Code.....38
Guy Edjlali (Wayne State University, USA)
Anurag Acharya (University of California, Santa Barbara, USA)
Vipin Chaudhary (Wayne State University, USA)

A Specification of Java Loading and Bytecode Verification.....49
Allen Goldberg (Kestrel Institute, USA)

Session 4: Cryptography

A New Public Key Cryptosystem Based on Higher Residues.....59
David Naccache (Gemplus Card International, France)
Jacques Stern (Ecole Normale Supérieure, France)

An Efficient Non-Interactive Statistical Zero-Knowledge Proof System for Quasi-Safe Prime Products...67
Rosario Gennaro (IBM T.J. Watson Research Center, USA)
Daniele Micciancio (MIT Laboratory for Computer Science, USA)
Tal Rabin (IBM T.J. Watson Research Center, USA)

Communication-Efficient Anonymous Group Identification.....73
Alfredo De Santis (Università di Salerno, Italy)
Giovanni Di Crescenzo (University of California San Diego, USA)
Giuseppe Persiano (Università di Salerno, Italy)

Session 5: Systems

A Security Architecture for Computational Grids.....83
Ian Foster (Argonne National Laboratory, USA)
Carl Kesselman and Gene Tsudik (USC Information Sciences Institute, USA)
Steven Tuecke (Argonne National Laboratory, USA)

Design of A High-Performance ATM Firewall.....93
Jun Xu and Mukesh Singhal (Ohio State University, USA)

A Practical Secure Physical Random Bit Generator.....103
Markus Jacobsson, Elizabeth Shriver, Bruce K. Hillyer (Bell Laboratories-Lucent Technologies, USA)
Ari Juels (RSA Labs, USA)

Session 6: Protocol Design and Analysis

A Probabilistic Poly-Time Framework for Protocol Analysis.....112
P. Lincoln (SRI International, USA)
J. Mitchell and M. Mitchell (Stanford University, USA)
A. Scedrov (University of Pennsylvania, USA)

Public-Key Cryptography and Password Protocols.....122
Shai Halevi (IBM T.J. Watson Research Center, USA)
Hugo Krawczyk (Technion, Israel and IBM T.J. Watson Research Center, USA)

Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP).....132
Bruce Schneier (Counterpane Systems, USA)
Mudge (L0pht Heavy Industries, USA)

Session 7: System Monitoring

How to Prove Where You Are: Tracking the Location of Customer Equipment.....142
Eran Gabber and Avishai Wool (Bell Laboratories-Lucent Technologies, USA)

Temporal Sequence Learning and Data Reduction for Anomaly Detection.....150
Terran Lane and Carla E. Brodley (Purdue University, USA)

Author Index.....159