Table of Contents

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

Intrusion Detection and Survivable Systems

The Base-Rate Fallacy and its Implication for Intrusion Detection 1
Stefan Axelsson (Chalmers Univ. Technology, Sweden)

A High-Performance Network Intrusion Detection System 8
R. Sekar, Y. Guang, S. Verma, T. Shanbag

The Proactive Security Toolkit and Applications 18
Boaz Barak, Amir Herzberg, Dalit Naor, Eldad Shai (IBM Research, Israel)

Cryptography

A Fuzzy Commitment Scheme 28
Ari Juels (RSA Labs, USA), Martin Wattenberg (USA)

On the Fly Signatures based on Factoring 37
Guillaume Poupard, Jacques Stern (École Normale Supérieure, France)

Signature Schemes Based on the Strong RSA Assumption 46
Ronald Cramer (ETH, Zurich), Victor Shoup (IBM Research, Switzerland)

Authentication

Proof-Carrying Authentication 52
Andrew Appel, Ed Felten (Princeton Univ. , USA)

Public-Key Cryptography and Password Protocols: The Multi-User Case 63
Maurizio Kliban Boyarsky (USA)

Password Hardening Based on Keystroke Dynamics 73
Fabian Monrose, Michael K. Reiter, Susanne Wetzel (Bell Labs, USA)

Group and Multicast Security

Secure Protocol Transformation via "Expansion" 83
Alain Mayer (Bell Labs, USA), Moti Yung (CertCo, USA)

A Compact and Fast Hybrid Signature Scheme for Multicast 93
Pankaj Rohatgi, (IBM T. J. Watson Research, USA)

Scalable Multicast Security in Dynamic Groups 101
Refik Molva, Alain Pannetrat (Institut Eurecom, France)

Anonymity

Anonymous Authentication with Subset Queries 113
Dan Boneh (Stanford Univ. , USA), Matt Franklin (Xerox PARC, USA)

Efficient Private Bidding and Auctions with an Oblivious Third Party ... 120
Christian Cachin (IBM Research, Switzerland)

Secure E-Commerce and Financial Cryptography

Using Smartcards to Secure a Personalized Gambling Device 128
William Aiello, Aviel Rubin, Martin Strauss (AT&T Labs, USA)

Efficient Verifiable Encryption (and Fair Exchange) of Digital Signatures 138
Giuseppe Ateniese (IBM Research, Switzerland; Univ. Genoa, Italy)

Author Index 147