Table of Contents

Symposium Committee ... viii

Steering Committee ... viii

Local Organizing Committee ... viii

Local Host and Co-Organizers ... viii

Program Committee ... ix

External Reviewers ... ix

Tutorial 1: Network Security and IPsec ... xi
J. Ioannidis (AT&T) and A. Keromytis (University of Pennsylvania)

Tutorial 2: Electronic Payment Technologies ... xii
Y. Frenkel (eCash Technologies)

Session 2-1: Certificate Management
Session Chair: *S. Stubblebine*

Evaluating Certificate Status Information Mechanisms ... 1
J. Iliadis, D. Spinellis, S. Katsikas (University of the Aegean),
D. Gritzalis (Athens University of Economics & Business), and B. Preneel (Universiteit Leuven)

Accountable Certificate Management using Undeniable Attestations ... 9
A. Buldas (Küberneetika AS), P. Laud (Universität des Saarlandes),
and H. Lipmaa (Helsinki University of Technology)

Efficient Fault-Tolerant Certificate Revocation ... 19
R. Wright (AT&T Labs–Research), P. Lincoln and J. Millen (SRI International)

Session 2-2: Privacy and Anonymity
Session Chair: *R. Wright*

Timing Attacks on Web Privacy ... 25
E. W. Felten and M. A. Schneider (Princeton University)

A Protocol for Anonymous Communication Over the Internet ... 33
C. Shields (Purdue University) and B. N. Levine (University of Massachusetts)

A Secure Execution Framework for Java ... 43
M. Hauswirth, C. Kerer, and R. Kurmanowytsch (Technical University of Vienna)

User Privacy Issues Regarding Certificates and the TLS Protocol (The Design and Implementation of the SPSL Protocol) 53
P. Persiano and I. Visconti (Università degli studi di Salerno)

Session 2-3: Electronic Commerce
Session Chair: *P. Spirakis*

Distribution Chain Security 63
G. Durfee (Stanford University) and M. Franklin (University of California, Davis)

Threshold-Based Identity Recovery for Privacy Enhanced Applications 71
J. Biskup and U. Flegel (University of Dortmund)

Reducing the Round Complexity of a Sealed-Bid Auction Protocol with Off-Line TTP 80
Y. Watanabe and H. Imai (University of Tokyo)

XML Document Security Based on Provisional Authorization 87
M. Kudo and S. Hada (IBM Research, Toyko Research Laboratory)

Invited Talk: Security: The State of the Practice 97
R. Ganesan (CheckFree Corporation)

Panel: Which PKI (Public Key Infrastructure) is the Right One? 98
C. Adams (Entrust Technologies), M. Burmester (Royal Holloway–University of London), Y. Desmedt (Florida State University), M. Reiter (Bell Labs, Lucent Technologies), and P. Zimmerman (PGP)

Session 3-1: Cryptography and Steganography
Session Chair: *B. Preneel*

Multi-Round Passive Attacks on Server-Aided RSA Protocols 102
J. Merkle (Secunet Security Networks AG)

Simple Forward-Secure Signatures From Any Signature Scheme 108
H. Krawczyk (Technion)

Moiré Cryptography 116
Y. Desmedt and T. V. Le (Florida State University)

Funkspiel Schemes: An Alternative to Conventional Tamper Resistance 125
J. Håstad (Royal Institute of Technology), J. Jonsson, A. Juels (RSA Laboratories), and M. Yung (CertCo, Inc.)

Session 3-2: Access Control
Session Chair: V. Varadharajan

Regulating Service Access and Information Release on the Web 134
P. Bonatti and P. Samarati (Università di Milano)

An Authorization Model for Temporal Data 144
A. Gal and V. Atluri (Rutgers University)

An Access Control Model for Simplifying Constraint Expression 154
J. E. Tidswell (University of New South Wales) and Trent Jaeger (IBM T.J. Watson Research Center)

A Modular Approach to Composing Access Control Policies 164
P. Bonatti (Università di Milano), S. De Capitani di Vimercati (Università di Brescia), and P. Samarati (Università di Milano)

Session 4-1: Systems Security
Session Chair: *E. Kiountouzis*

Operating System Enhancements to Prevent the Misuse of System Calls 174
M. Bernaschi, E. Gabrielli (IAC-CNR), and L. V. Mancini (Università di Roma "La Sapienza")

Using Router Stamping to Identify the Source of IP Packets 184
T. W. Doeppner, P. N. Klein (Brown University), A. Koyfman (Oracle Corporation)

Implementing a Distributed Firewall 190
S. Ioannidis, A. D. Keromytis (University of Pennsylvania), S. Bellovin (AT&T Labs–Research), and J. M. Smith (University of Pennsylvania)

Security Enhanced Mobile Agents 200
V. Varadharajan (University of West Sydney)

Session 4-2: Internet Security and Composition
Session Chair: T. Apostolopoulos

PRUNES: An Efficient and Complete Strategy for Automated Trust Negotiation over the Internet 210
T. Yu, X. Ma, and M. Winslett (University of Illinois at Urbana-Champaign)

Cross Domain One-Shot Authorization using Smart Cards 220
R. Au, M. Looi (Queensland University of Technology), and P. Ashley (Tivoli, Security Business Unit)

New Constructions for Multicast Re-keying Schemes using Perfect Hash Families 228
R. Safavi-Naini and H. Wang (University of Wollongong)

Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups 235
Y. Kim (University of Southern California), A. Perring (University of California at Berkeley), and G. Tsudik (University of California at Irvine)

Composition and Integrity Preservation of Secure Reactive Systems 245
B. Pfitzmann (Univerität des Saarlandes) and M. Waidner (IBM Research Division)

Author Index 255