Table of Contents

Risk Management

Developing Electronic Trust Policies Using a Risk Management Model 1
Dean Povey

Security Design

SECURE: A Simulation Tool for PKI Design 17
Luigi Romano, Antonino Mazzeo, Nicola Mazzocca

Lazy Infinite-State Analysis of Security Protocols 30
David Basin

Electronic Payment

Electronic Payments – Where Do We Go from Here? 43
Moti Yung, Yiannis Tsiounis, Markus Jakobsson, David MRaihi

SmartCard Issues

PCA: Jini-based Personal Card Assistant 64
Roger Kehr, Joachim Posegga, Harald Vogt

An X.509-Compatible Syntax for Compact Certificates 76
Magnus Nyström, John Brainard

Applications

Secure and Cost Efficient Electronic Stamps 94
Detlef Hühnlein, Johannes Merkle

Implementation of a Digital Lottery Server on WWW 101
Kazue Sako

PKI-experiences (Workshop Notes)

Cert’eM: Certification System Based on Electronic Mail Service Structure 109
Javier Lopez, Antonio Mana, Juan J. Ortega

A Method for Developing Public Key Infrastructure Models....................................119
Klaus Schmeh

The Realities of PKI Inter-operability 127
John Hughes

Mobile Security

Mobile Security – An Overview of GSM, SAT and WAP 133
Malte Borcherding

Secure Transport of Authentication Data in Third Generation Mobile Phone Networks 142
Stefan Pütz, Roland Schmitz, Benno Tietz

Cryptography

Extending Wiener’s Attack in the Presence of Many Decrypting Exponents............153
Jean-Pierre Seifert, Nick Howgrave-Graham

Improving the Exact Security of Fiat-Shamir Signature Schemes.............................167
Silvio Micali, Leonid Reyzin

Network Security (Workshop Notes)

On Privacy Issues of Internet Access Services via Proxy Servers 183
Yuen-Yan Chan

Cryptanalysis of Microsoft’s PPTP Authentication Extensions (MS-CHAPv2)........192
Bruce Schneier, Mudge, David Wagner

Key Recovery

Auto-recoverable Auto-certifiable Cryptosystems (A Survey)..................................204
Moti Yung, Adam Young

Intrusion Detection

A Distributed Intrusion Detection System Based on Bayesian Alarm Networks.......219
Dusan Bulatovic, Dusan Velasevic

Interoperability

Interoperability Characteristics of S/MIME Products..229
Sarbari Gupta, Jerry Mulvenna, Srivinas Ganta, Larry Keys, Dale Walters

The DEDICA Project: The Solution to the Interoperability Problems between the X.509 and EDIFACT Public Key Infrastructures..242
Montse Rubia, Juan Carlos Cruellas, Manel Medina

Biometrics

Multiresolution Analysis and Geometric Measures for Biometric Identification Systems..251
Raul Sanchez-Reillo, Carmen Sanchez-Avila, Ana Gonzales-Marco

Author Index..259

Dates and Deadlines of CQRE [Secure] 2000...261