

Table of Contents

Risk Management

Developing Electronic Trust Policies Using a Risk Management Model	1
<i>Dean Povey</i>	

Security Design

SECURE: A Simulation Tool for PKI Design.....	17
<i>Luigi Romano, Antonino Mazzeo, Nicola Mazzocca</i>	
Lazy Infinite-State Analysis of Security Protocols	30
<i>David Basin</i>	

Electronic Payment

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

SmartCard Issues

PCA: Jini-based Personal Card Assistant	64
<i>Roger Kehr, Joachim Posegga, Harald Vogt</i>	
An X.509-Compatible Syntax for Compact Certificates	76
<i>Magnus Nyström, John Brainard</i>	

Applications

Secure and Cost Efficient Electronic Stamps	94
<i>Detlef Hühnlein, Johannes Merkle</i>	
Implementation of a Digital Lottery Server on WWW	101
<i>Kazuo Sako</i>	

PKI-experiences (Workshop Notes)

Cert'eM: Certification System Based on Electronic Mail Service Structure109
Javier Lopez, Antonio Mana, Juan J. Ortega

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

The Realities of PKI Inter-operability127
John Hughes

Mobile Security

Mobile Security – An Overview of GSM, SAT and WAP133
Malte Borcharding

Secure Transport of Authentication Data in Third Generation Mobile Phone
Networks142
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 Servers183
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
<i>Dusan Bulatovic, Dusan Velasevic</i>	

Interoperability

Interoperability Characteristics of S/MIME Products.....	229
<i>Sarbari Gupta, Jerry Mulvenna, Srivinas Ganta, Larry Keys, Dale Walters</i>	
The DEDICA Project: The Solution to the Interoperability Problems between the X.509 and EDIFACT Public Key Infrastructures	242
<i>Montse Rubia, Juan Carlos Cruellas, Manel Medina</i>	

Biometrics

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

Author Index	259
---------------------------	-----

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

<http://www.springer.com/978-3-540-66800-8>

Secure Networking - CQRE (Secure) '99
International Exhibition and Congress Düsseldorf,
Germany, November 30 - December 2, 1999,
Proceedings
Baumgart, R. (Ed.)
1999, X, 266 p., Softcover
ISBN: 978-3-540-66800-8