Preface

The CQRE [Secure] conference provides a new international forum giving a close-up view on information security in the context of rapidly evolving economic processes. The unprecedented reliance on computer technology has transformed the previous technical side-issue "information security" to a management problem requiring decisions of strategic importance. Thus one of the main goals of the conference is to provide a platform for both technical specialists as well as decision makers from government, industry, commercial, and academic communities. The target of CQRE is to promote and stimulate dialogue between managers and experts, which seems to be necessary for providing secure information systems in the next millennium.

Therefore CQRE consists of two parts: Part I mainly focuses on strategic issues of information security, while the focus of Part II is more technical in nature. This volume of the conference proceedings consists of the reviewed and invited contributions of the second part.

The program committee considered 46 papers and selected only 15 for full presentation. For the participants’ convenience we have also included the notes of the invited lectures and short workshop talks in this volume.

The selection of papers was a difficult and challenging task. I wish to thank the program committee members who indeed did an excellent job in reviewing and selecting the papers and providing useful feedback to authors. Each submission was blindly refereed by at least three reviewers to make the selection process as fair and objective as possible. The program committee was assisted by many colleagues who reviewed submissions in their field of expertise. My thanks to all of them.

I would also like to thank the entire CQRE-team for their kind assistance in organizing this event. My special thanks to our hosts from Messe-Düsseldorf GmbH and especially to N. Mizera, M. Kotschedoff, S. Spamer, A. Viefers, and B. Wagner who greatly contributed to the success of this challenging project with their untiring engagement and timely decisions. Furthermore I would like to thank the team from Brodeur-Kohtes & Klewes around B. Boendel and my colleagues T. Gawlick, A. M. Schlesinger, and D. Hühnlein for kindly assisting me in administrative tasks.

Last but not least, I wish to thank all the authors who submitted papers, making this conference possible, and the authors of accepted papers for updating their work in a timely manner, allowing the production of these proceedings.

September 1999

Rainer Baumgart
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
VIII Table of Contents

**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 Gonzalez-Marco

Author Index.............................................................................................................259

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