

# Contents

## Measures

|                                           |   |
|-------------------------------------------|---|
| Valuation of Trust in Open Networks ..... | 3 |
| <i>T. Beth, M. Borchering, B. Klein</i>   |   |

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Security Versus Performance Requirements<br>in Data Communication Systems ..... | 19 |
| <i>V. Zorkadis</i>                                                              |    |

## High Assurance Software

|                                              |    |
|----------------------------------------------|----|
| Non-Interference Through Determinism .....   | 33 |
| <i>A.W. Roscoe, J.C.P. Woodcock, L. Wulf</i> |    |

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Compile-Time Detection of Information Flow in Sequential Programs ..... | 55 |
| <i>J.-P. Banâtre, C. Bryce, D. Le Métayer</i>                           |    |

|                                      |    |
|--------------------------------------|----|
| Security Through Type Analysis ..... | 75 |
| <i>C. O'Halloran, C.T. Sennett</i>   |    |

## Key Management I

|                                               |    |
|-----------------------------------------------|----|
| Designing Secure Key Exchange Protocols ..... | 93 |
| <i>C. Boyd, W. Mao</i>                        |    |

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| Robust and Secure Password and Key Change Method .....               | 107 |
| <i>R. Hauser, P. Janson, R. Molva, G. Tsudik, E. Van Herreweghen</i> |     |

## Authentication

|                                      |     |
|--------------------------------------|-----|
| Beacon Based Authentication .....    | 125 |
| <i>A. Jiwa, J. Seberry, Y. Zheng</i> |     |

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| Authentication via Multi-Service Tickets in the Kuperee Server ..... | 143 |
| <i>T. Hardjono, J. Seberry</i>                                       |     |

|                            |     |
|----------------------------|-----|
| Oblivious Signatures ..... | 161 |
| <i>L. Chen</i>             |     |

## Key Management II

- A Calculus for Secure Channel Establishment in Open Networks ..... 175  
*U.M. Maurer, P.E. Schmid*
- On Strengthening Authentication Protocols to Foil Cryptanalysis ..... 193  
*W. Mao, C. Boyd*

## Digital Payment

- An Efficient Electronic Payment System Protecting Privacy ..... 207  
*J.L. Camenisch, J.M. Piveteau, M.A. Stadler*
- The ESPRIT Project CAFE - High Security Digital Payment Systems ... 217  
*J.-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjølsnes,  
 F. Muller, T. Pedersen, B. Pfitzmann, P. de Rooij, B. Schoenmakers,  
 M. Schunter, L. Vallée, M. Waidner*
- Liability and Computer Security: Nine Principles ..... 231  
*R.J. Anderson*

## Distributed Systems

- Implementing Secure Dependencies over a Network by Designing  
 a Distributed Security SubSystem ..... 249  
*B. d'Ausbourg*
- A Secure Medium Access Control Protocol: Security vs Performances .... 267  
*P. Siron, B. d'Ausbourg*
- Distributed File System over a Multilevel Secure Architecture -  
 Problems and Solutions ..... 281  
*C. Calas*

## Access Controls

- On the Expressive Power of the Unary Transformation Model ..... 301  
*R.S. Sandhu, S. Ganta*
- Privilege Graph: an Extension to the Typed Access Matrix Model ..... 319  
*M. Dacier, Y. Deswarte*
- A Consideration of the Modes of Operation for Secure Systems ..... 335  
*C.L. Robinson, S.R. Wiseman*

## Database I

|                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------|-----|
| Mark-and-Sweep Garbage Collection in Multilevel Secure<br>Object-Oriented Database Systems .....                 | 359 |
| <i>A. Ciampichetti, E. Bertino, L. Mancini</i>                                                                   |     |
| Decomposition of Multilevel Objects in an Object-Oriented Database ....                                          | 375 |
| <i>N. Boulahia-Cuppens, F. Cuppens, A. Gabillon, K. Yazdanian</i>                                                |     |
| Supporting Object-Based High-Assurance Write-up in Multilevel<br>Databases for the Replicated Architecture ..... | 403 |
| <i>R.K. Thomas, R.S. Sandhu</i>                                                                                  |     |

## Database II

|                                                                                              |     |
|----------------------------------------------------------------------------------------------|-----|
| Aggregation in Relational Databases: Controlled Disclosure<br>of Sensitive Information ..... | 431 |
| <i>A. Motro, D.G. Marks, S. Jajodia</i>                                                      |     |
| Information Flow Controls vs Interference Controls:<br>An Integrated Approach .....          | 447 |
| <i>F. Cuppens, G. Trouessin</i>                                                              |     |
| List of Authors .....                                                                        | 469 |