

Contents

Access Control

- Towards Security in an Open Systems Federation 3
John A. Bull, Li Gong, Karen R. Sollins
- Type-Level Access Controls for Distributed Structurally
Object-Oriented Database Systems 21
Udo Kelter
- On the Chinese Wall Model 41
Volker Kessler

Formal Methods

- Formal Methods and Automated Tool for Timing-Channel
Identification in TCB Source Code 57
Jingsha He, Virgil D. Gligor
- Separating the Specification and Implementation Phases in
Cryptology 77
Marie-Jeanne Toussaint
- Formal Specification of Security Requirements using the
Theory of Normative Positions 103
Andrew J.I. Jones, Marek Sergot

Invited Talk

- Breaking the Traditional Computer Security Barriers 125
Yvo Desmedt

Authentication I

Verification and Modelling of Authentication Protocols <i>Ralf C. Hauser, E. Stewart Lee</i>	141
KryptoKnight Authentication and Key Distribution System <i>Refik Molva, Gene Tsudik, Els Van Herreweghen, Stefano Zatti</i>	155
Associating Metrics to Certification Paths <i>Anas Tarah, Christian Huitema</i>	175

Distributed Systems

An Object-Oriented View of Fragmented Data Processing for Fault and Intrusion Tolerance in Distributed Systems <i>Jean-Charles Fabre, Brian Randell</i>	193
The Development and Testing of the Identity-Based Conference Key Distribution System for the RHODOS Distributed System <i>Michael Wang, Andrzej Goscinski</i>	209
Policy Enforcement in Stub Autonomous Domains <i>Gene Tsudik</i>	229

Authentication II

Freshness Assurance of Authentication Protocols <i>Kwok-Yan Lam, Dieter Gollmann</i>	261
A Formal Framework for Authentication <i>Colin Boyd</i>	273
Timely Authentication in Distributed Systems <i>Kwok-Yan Lam, Thomas Beth</i>	293

Database Security

Polyinstantiation for Cover Stories <i>Ravi S. Sandhu, Sushil Jajodia</i>	307
On Transaction Processing for Multilevel Secure Replicated Databases <i>Iwen E. Kang, Thomas F. Keefe</i>	329
Security Constraint Processing in Multilevel Secure AMAC Schemata <i>Günther Pernul</i>	349

System Architectures

M ² S: A Machine for Multilevel Security <i>Bruno d'Ausbourg, Jean-Henri Llaureus</i>	373
GDoM: a Multilevel Document Manager <i>Christel Calas</i>	393

Applications

UEPS — A Second Generation Electronic Wallet <i>Ross J. Anderson</i>	411
A Hardware Design Model for Cryptographic Algorithms <i>Joan Daemen, René Govaerts, Joos Vandewalle</i>	419
ASAX: Software Architecture and Rule-Based Language for Universal Audit Trail Analysis <i>Naji Habra, Baudouin Le Charlier, Abdelaziz Mounji, Isabelle Mathieu</i>	435

Author Index	451
--------------	-----