Table of Contents

Fixed vs. Variable-Length Patterns for Detecting Suspicious Process Behavior ................................................................. 1
   H. Debar, M. Dacier, M. Nassehi, and A. Wespi

A Tool for Pro-active Defense Against the Buffer Overrun Attack ...... 17
   D. Bruschi, E. Rosti, and R. Banfi

A Kernelized Architecture for Multilevel Secure Application Policies . . . 33
   S.N. Foley

Dealing with Multi-policy Security in Large Open Distributed Systems . . 51
   C. Bidan and V. Issarny

   R. Ortao

On the Security of Some Variants of the RSA Signature Scheme .......... 85
   M. Michels, M. Stadler, and H.-M. Sun

Side Channel Cryptanalysis of Product Ciphers ............................. 97
   J. Kelsey, B. Schneier, D. Wagner, and C. Hall

On the Security of Digital Tachographs .................................... 111
   R. Anderson

An Authorization Model and Its Formal Semantics .......................... 127
   E. Bertino, F. Buccafurri, E. Ferrari, and P. Rullo

Authorization in CORBA Security ............................................ 143
   G. Karjoth

Rules for Designing Multilevel Object-Oriented Databases................. 159
   F. Cuppens and A. Gabillon

Byte Code Verification for Java Smart Cards Based on Model Checking . 175
   J. Posegga and H. Vogt

Towards Formalizing the Java Security Architecture of JDK 1.2 .......... 191
   L. L. Kassab and S. J. Greenwald

EUROMED-JAVA: Trusted Third Party Services for Securing Medical Java Applets .............................................................. 209
   A. Varvitsiotis, D. Polemi, and A. Marsh
MPEG PTY-Marks: Cheap Detection of Embedded Copyright Data in DVD-Video ...................................................... 221
  J.P.M.G. Linnartz and J.C. Talstra

DHWM: A Scheme for Managing Watermarking Keys in the Aquarelle Multimedia Distributed System .................................... 241
  D. Augot, J.-F. Delaigle, and C. Fontaine

The Ticket Concept for Copy Control Based on Embedded Signalling . 257
  J.P.M.G. Linnartz

Panel Session: Watermarking ............................................ 275
  G. Eizenberg and J.-J. Quisquater

Authentication and Payment in Future Mobile Systems ................. 277
  G. Horn and B. Preneel

Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks ........... 295
  D. Kesdogan, P. Reichl, and K. Junghärtchen

A Mix-Mediated Anonymity Service and Its Payment .................. 313
  E. Franz and A. Jerichow

A Subjective Metric of Authentication ................................... 329
  A. Jøsang

A Sound Logic for Analysing Electronic Commerce Protocols ........... 345
  V. Kessler and H. Neumann

Kerberos Version IV: Inductive Analysis of the Secrecy Goals ........ 361
  G. Bella and L.C. Paulson

Author Index .............................................................. 377