Table of Contents

Biometrics

Biometric Authentication in Infrastructure Security 1
John Armington, Purdy Ho, Paul Koznek, Richard Martinez

Denial of Access in Biometrics-Based Authentication Systems 19
Luciano Rila

Identification, Authentication, and Process

A Novel Approach to Proactive Password Checking 30
Carlo Blundo, Paolo D'Arco, Alfredo De Santis, Clemente Galdi

Single Sign-On Architectures 40
Jan De Clercq

Active Digital Credentials: Dynamic Provision of Up-to-Date Identity Information 59
Marco Casassa Mont, Richard Brown

Analysis Process

How to Buy Better Testing (Using Competition to Get the Most Security and Robustness for Your Dollar) 73
Stuart Schechter

Structured Risk Analysis 88
Neil McEvoy, Andrew Whitcombe

A Model Enabling Law Compliant Privacy Protection through the Selection and Evaluation of Appropriate Security Controls 104
E.S. Siougle, V.C. Zorkadis

Mobile Networks

Authentication and Authorization of Mobile Clients in Public Data Networks 115
Prakash Reddy, Venky Krishnan, Kan Zhang, Devaraj Das

A Contemporary Foreword on GSM Security 129
Paulo S. Pagliusi

Vulnerability Assessment and Logs

Vulnerability Assessment Simulation for Information Infrastructure Protection 145
HyungJong Kim, KyungHee Koh, DongHoon Shin, HongGeun Kim

Pseudonymizing Unix Log Files. 162
Ulrich Flegel

System Design

DPS: An Architectural Style for Development of Secure Software 180
Pascal Fenkam, Harald Gall, Mehdi Jazayeri, Christopher Kruegel

A New Infrastructure for User Tracking Prevention and Privacy Protection in Internet Shopping 199
Matthias Enzmann, Thomas Kunz, Markus Schneider

Different Smartcard-Based Approaches to Physical Access Control 214
Óscar Cánovas, Antonio F. Gómez, Humberto Martínez, Gregorio Martínez

Formal Methods

Authenticity and Provability – A Formal Framework 227
Sigrid Gürgens, Peter Ochsenschläger, Carsten Rudolph

Protocol Engineering Applied to Formal Analysis of Security Systems 246
Javier Lopez, Juan J. Ortega, Jose M. Troya

Cryptographic Techniques

Applications of Multiple Trust Authorities in Pairing Based Cryptosystems 260
L. Chen, K. Harrison, D. Soldera, N.P. Smart

Plausible Deniability Using Automated Linguistic Stegonagraphy 276
Mark Chapman, George Davida

Virtual Software Tokens – A Practical Way to Secure PKI Roaming 288
Taekyoung Kwon

Bit-Serial AOP Arithmetic Architectures over $GF(2m)$ 303
Hyun-Sung Kim, Kee-Young Yoo

Networks

A Practical Distributed Authorization System for GARA 314
William A. Adamson, Olga Kornievskaia

Design of a VPN Software Solution Integrating TCP and UDP Services ... 325
Javier Lopez, Jose A. Montenegro, Rodrigo Roman, Jorge Davila

Author Index 339