### Table of Contents

#### Invited Talk

Developing Secure, Trusted and Auditable Services for e-Business: An Autonomic Computing Approach ...................................................... 1  
*Ahmed Patel*

#### Trust

A Mechanism for Trust Sustainability Among Trusted Computing Platforms .... 11  
*Zheng Yan and Piotr Cofia*

Enabling Trust-Awareness in Naming Services ................................. 20  
*Nicola Mezzetti*

Virtual Trust in Distributed Systems ............................................... 30  
*Semir Daskapan, Ana Cristina Costa, Willem G. Vree, and Amr A. Eldin*

Modelling Trust Relationships in Distributed Environments ............... 40  
*Weiliang Zhao, Vijay Varadharajan, and George Bryan*

#### Access Control

Dynamically Changing Trust Structure in Capability Based Access Control Systems .......................................................... 50  
*Sandra Wortmann, Barbara Sprick, and Christoph Kobusch*

On the Design of a New Trust Model for Mobile Agent Security ............ 60  
*Ching Lin, Vijay Varadharajan, Yan Wang, and Yi Mu*

#### e-Business Issues

Balancing Privacy and Trust in Electronic Marketplaces ..................... 70  
*Sandra Steinbrecher*

Reducing Server Trust in Private Proxy Auctions ............................. 80  
*Giovanni Di Crescenzo, Javier Herranz, and Germán Sáez*

Secure Ad-Hoc mBusiness: Enhancing WindowsCE Security ............... 90  
*Florina Alménarez, Daniel Díaz, and Andrés Martín*

Role-Based Privilege Management Using Attribute Certificates and Delegation . 100  
*Gail-Joon Ahn, Dongwan Shin, and Longhua Zhang*
# Table of Contents

## Privacy

Consent as a Threat. A Critical Approach to Privacy Negotiation in e-Commerce Practices ............................................. 110  
* A. Daniel Oliver-Lalana

Dealing with Privacy Obligations: Important Aspects and Technical Approaches . 120  
* Marco Casassa Mont

Offer Privacy in Mobile Agents  
Using Conditionally Anonymous Digital Signatures ........................ 132  
* Ming Yao, Matt Henrickson, Ernest Foo, and Ed Dawson

Privacy Preserving Data Generation  
for Database Application Performance Testing ................................. 142  
* Yongge Wang, Xintao Wu, and Yuliang Zheng

## e-Voting

An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness ............ 152  
* Riza Aditya, Byoungcheon Lee, Colin Boyd, and Ed Dawson

Trust in Public Administration e-Transactions: e-Voting in the UK .............. 162  
* Alexandros Xenakis and Ann Macintosh

## Protocols

An Unbalanced Protocol for Group Key Exchange ................................. 172  
* Javier Herranz and Jorge L. Villar

Certified E-Mail with Temporal Authentication:  
An Improved Optimistic Protocol .................................................. 181  
* Clemente Galdi and Raffaella Giordano

Efficient Password-Based Group Key Exchange ................................. 191  
* Su Mi Lee, Jung Yeon Hwang, and Dong Hoon Lee

Optimality in Asynchronous Contract Signing Protocols .......................... 200  
* Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, and Llorenç Huguet-Rotger

## Copyright Protection

Development of Visible Anti-copy Patterns ...................................... 209  
* JongWeon Kim, KyuTae Kim, JungSoo Lee, and JongUk Choi
Holographic Image Watermarking for Secure Content .......................... 219  
KyuTae Kim, JongWeon Kim, JungSoo Lee, and JongUk Choi

Hybrid Fingerprint Matching on Programmable Smart Cards .......... 232  
Tommaso Cucinotta, Riccardo Brigo, and Marco Di Natale

Protecting ASF Movie on VOD ................................................. 242  
Ji-Hyun Park, Jeong-Hyun Kim, and Ki-Song Yoon

Multicast

DiffSig: Differentiated Digital Signature for Real-Time Multicast Packet Flows . . 251  
Namhi Kang and Christoph Ruland

Large-Scale Pay-As-You-Watch for Unicast and Multicast Communications .... 261  
Antoni Martínez-Ballesté, Francesc Sebé, and Josep Domingo-Ferrer

PKI, Signature Schemes

Reducing the Communication Overhead of an Offline Revocation Dictionary . . . 269  
Jose L. Muñoz, Jordi Forné, Oscar Esparza, Josep Pegueroles,  
and Esteve Pallarès

Tommaso Cucinotta, Marco Di Natale, and David Corcoran

On the Security of the Lee-Hwang Group-Oriented  
Undeniable Signature Schemes .............................................. 289  
Guilin Wang, Jianying Zhou, and Robert H. Deng

Author Index ............................................................................ 299