Table of Contents

Invited Talks (Abstracts)

The Age of Pervasive Computing – Everything Smart, Everything Connected? … 1
Friedemann Mattern

Cyber Assist Project and Its Security Requirement ……………………. 2
Hideyuki Nakashima

Security in Pervasive Computing ………………………………….. 6
Frank Stajano

The Importance of High Assurance Security in Pervasive Computing ……… 9
Paul A. Karger

Location Privacy

A Methodological Assessment of Location Privacy Risks
in Wireless Hotspot Networks ………………………………………….. 10
Marco Gruteser and Dirk Grunwald

Protecting Access to People Location Information ……………………. 25
Urs Hengartner and Peter Steenkiste

Security Requirements

Smart Devices and Software Agents: The Basics of Good Behaviour ……… 39
Howard Chivers, John A. Clark, and Susan Stepney

Dependability Issues of Pervasive Computing in a Healthcare Environment ….. 53
Jürgen Bohn, Felix Gärtner, and Harald Vogt

Security Policies and Protection

Protecting Security Policies in Ubiquitous Environments
Using One-Way Functions …………………………………………….. 71
Håkan Kvarnström, Hans Hedbom, and Erland Jonsson

Enforcing Security Policies via Types ………………………………. 86
Daniele Gorla and Rosario Pugliese

Towards Using Possibilistic Information Flow Control
to Design Secure Multiagent Systems ……………………………... 101
Axel Schairer
### Authentication and Trust

**Authentication for Pervasive Computing** ........................................ 116  
_Sadie Creese, Michael Goldsmith, Bill Roscoe, and Irfan Zakiuddin_

**End-to-End Trust Starts with Recognition** .................................... 130  
_Jean-Marc Seigneur, Stephen Farrell, Christian Damsgaard Jensen, Elizabeth Gray, and Yong Chen_

**Embedding Distance-Bounding Protocols within Intuitive Interactions** ........ 143  
_Laurent Bussard and Yves Roudier_

### Secure Infrastructures

**Trust Context Spaces: An Infrastructure for Pervasive Security in Context-Aware Environments** .................................................. 157  
_Philip Robinson and Michael Beigl_

**Time Constraint Delegation for P2P Data Decryption** .................... 173  
_Tie-Yan Li_

**SAOTS: A New Efficient Server Assisted Signature Scheme for Pervasive Computing** .................................................. 187  
_Kemal Bicakci and Nazife Baykal_

### Smart Labels

**Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems** .................................................. 201  
_Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels_

### Verification

**Implementing a Formally Verifiable Security Protocol in Java Card** ........ 213  
_Engelbert Hubbers, Martijn Oostdijk, and Erik Poll_

### Hardware Architectures

**Cellular Automata Based Multiplier for Public-Key Cryptosystem** .......... 227  
_Hyun-Sung Kim and Kee-Young Yoo_

**Enlisting Hardware Architecture to Thwart Malicious Code Injection** ........ 237  
_Ruby B. Lee, David K. Karig, John P. McGregor, and Zhijie Shi_

**Optimized RISC Architecture for Multiple-Precision Modular Arithmetic** ........ 253  
_Johann Großschädl and Guy-Armand Kamendje_

**Visual Crypto Displays Enabling Secure Communications** ................. 271  
_Pim Tuyls, Tom Kevenaar, Geert-Jan Schrijen, Toine Staring, and Marten van Dijk_
Workshop

Security and Privacy in Pervasive Computing State of the Art
and Future Directions .................................................. 285

Dieter Hutter, Werner Stephan, and Markus Ullmann

Author Index ............................................................ 291