

Table of Contents

Invited Talks (Abstracts)

The Age of Pervasive Computing – Everything Smart, Everything Connected? . . .	1
<i>Friedemann Mattern</i>	
Cyber Assist Project and Its Security Requirement	2
<i>Hideyuki Nakashima</i>	
Security in Pervasive Computing	6
<i>Frank Stajano</i>	
The Importance of High Assurance Security in Pervasive Computing	9
<i>Paul A. Karger</i>	

Location Privacy

A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks	10
<i>Marco Gruteser and Dirk Grunwald</i>	
Protecting Access to People Location Information	25
<i>Urs Hengartner and Peter Steenkiste</i>	

Security Requirements

Smart Devices and Software Agents: The Basics of Good Behaviour	39
<i>Howard Chivers, John A. Clark, and Susan Stepney</i>	
Dependability Issues of Pervasive Computing in a Healthcare Environment	53
<i>Jürgen Bohn, Felix Gärtner, and Harald Vogt</i>	

Security Policies and Protection

Protecting Security Policies in Ubiquitous Environments Using One-Way Functions	71
<i>Håkan Kvarnström, Hans Hedbom, and Erland Jonsson</i>	
Enforcing Security Policies via Types	86
<i>Daniele Gorla and Rosario Pugliese</i>	
Towards Using Possibilistic Information Flow Control to Design Secure Multiagent Systems	101
<i>Axel Schairer</i>	

Authentication and Trust

Authentication for Pervasive Computing	116
<i>Sadie Creese, Michael Goldsmith, Bill Roscoe, and Irfan Zakiuddin</i>	
End-to-End Trust Starts with Recognition	130
<i>Jean-Marc Seigneur, Stephen Farrell, Christian Damsgaard Jensen, Elizabeth Gray, and Yong Chen</i>	
Embedding Distance-Bounding Protocols within Intuitive Interactions	143
<i>Laurent Bussard and Yves Roudier</i>	

Secure Infrastructures

Trust Context Spaces: An Infrastructure for Pervasive Security in Context-Aware Environments	157
<i>Philip Robinson and Michael Beigl</i>	
Time Constraint Delegation for P2P Data Decryption	173
<i>Tie-Yan Li</i>	
SAOTS: A New Efficient Server Assisted Signature Scheme for Pervasive Computing	187
<i>Kemal Bicakci and Nazife Baykal</i>	

Smart Labels

Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems	201
<i>Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels</i>	

Verification

Implementing a Formally Verifiable Security Protocol in Java Card	213
<i>Engelbert Hubbers, Martijn Oostdijk, and Erik Poll</i>	

Hardware Architectures

Cellular Automata Based Multiplier for Public-Key Cryptosystem	227
<i>Hyun-Sung Kim and Kee-Young Yoo</i>	
Enlisting Hardware Architecture to Thwart Malicious Code Injection	237
<i>Ruby B. Lee, David K. Karig, John P. McGregor, and Zhijie Shi</i>	
Optimized RISC Architecture for Multiple-Precision Modular Arithmetic	253
<i>Johann Großschädl and Guy-Armand Kamendje</i>	
Visual Crypto Displays Enabling Secure Communications	271
<i>Pim Tuyls, Tom Kevenaar, Geert-Jan Schrijen, Toine Staring, and Marten van Dijk</i>	

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