Lecture Notes in Computer Science 2802

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Dieter Hutter Günter Müller
Werner Stephan Markus Ullmann (Eds.)

Security in Pervasive Computing

First International Conference
Boppard, Germany, March 12-14, 2003
Revised Papers

Springer

Volume Editors

Dieter Hutter
Werner Stephan
German Research Centre for Artificial Intelligence, DFKI
Stuhlsatzenhausweg 3, 66123 Saarbrücken, Germany
E-mail: {hutter,stephan}@dfki.de

Günter Müller
University of Freiburg, Institute for Computer Science
Friedrichstrasse 50, 79098 Freiburg, Germany
E-mail: mueller@iig.uni-freiburg.de

Markus Ullmann
BSI
Godesberger Allee 183, 53175 Bonn, Germany
E-mail: Markus.Ullmann@bsi.bund.de

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): C.2, D.2, D.4.6, H.5, K.4.1, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-20887-9 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10980521 06/3142 5 4 3 2 1 0

Preface

The ongoing compression of computing facilities into small and mobile devices like handhelds, portables or even wearable computers will enhance ubiquitous information processing. The basic paradigm of such pervasive computing is the combination of strongly decentralized and distributed computing with the help of diversified devices allowing for spontaneous connectivity via the Internet. Computers will become invisible to the user, and exchange of information between devices will effectively be beyond the user's control.

Assuming a broad usage of more powerful tools and more effective ways to use them the quality of everyday life will be strongly influenced by the dependability of the new technology. Information stored, processed, and transmitted by the various devices is one of the most critical resources. Threats exploiting vulnerabilities of new kinds of user interfaces, displays, operating systems, networks, and wireless communications will cause new risks of losing confidentiality, integrity, and availability. Can these risks be reduced by countermeasures to an acceptable level or do we have to redefine political and social demands.

The objective of this 1st International Conference on Security in Pervasive Computing was to develop new security concepts for complex application scenarios based on systems like handhelds, phones, smartcards, and smart labels hand in hand with the emerging technology of ubiquitous and pervasive computing. Particular subjects were methods and technology concerning the identification of risks, the definition of security policies, and the development of security measures that are related to the specific aspects of ubiquitous and pervasive computing like mobility, communication, and secure hardware/software platforms.

We received 51 submissions. Each submission was reviewed by three independent reviewers and an electronic program committee meeting was held via the Internet. We are very grateful to the program committee members for their efficency in processing the work within four weeks and also for the quality of their reviews and discussions. Finally the program committee decided to accept 19 papers. We are also very grateful to the four invited speakers for their vivid and stimulating talks.

Apart from the program committee, we would like to thank also the other persons who contributed to the success of this conference: the additional referees for reviewing the papers, the authors for submitting the papers, and the local organizers, and in particular Hans-Peter Wagner, for a smooth and pleasant stay in Boppard.

June 2003

Dieter Hutter, Günter Müller,
Werner Stephan, Markus Ullmann
Program Co-chairs SPC 2003

Organization

SPC 2003 was organized by the German Research Center for Artificial Intelligence in Saarbrücken and the German Bundesamt für Sicherheit in der Informationstechnik in Bonn.

Executive Committee

Program Co-chairs	Dieter Hutter (DFKI GmbH, Germany)
	Günter Müller (University of Freiburg, Germany)
	Werner Stephan (DFKI GmbH, Germany)
	Markus Ullmann (BSI, Germany)
Local Arrangements	Hans-Peter Wagner (BSI, Germany)

Program Committee

Michael Beigl	University of Karlsruhe, Germany
Joshua Guttman	MITRE, USA
Dieter Hutter	DFKI Saarbrücken, Germany
Paul Karger	IBM Watson Research, USA
Friedemann Mattern	ETH Zürich, Switzerland
Catherine Meadows	Naval Research Lab, USA
Guenter Mueller	University of Freiburg, Germany
Joachim Posegga	SAP, Germany
Kai Rannenberg	University of Frankfurt, Germany
Kurt Rothermel	University of Stuttgart, Germany
Ryoichi Sasaki	Tokyo Denki University, Japan
Frank Stajano	Cambridge University, UK
Werner Stephan	DFKI Saarbrücken, Germany
Moriyasu Takashi	Hitachi Ltd., Japan
Seiji Tomita	NTT Information Platform Laboratories, Japan
Markus Ullmann	BSI, Bonn, Germany

Invited Speakers

Friedemann Mattern	ETH Zürich, Switzerland
Hideyuki Nakashima	Cyber Assist Research Center, AIST, Japan
Frank Stajano	Cambridge University, UK
Markus Luidolt	Philips Semiconductors, Austria
Paul Karger	IBM Watson Research, USA

Additional Referees

L. Fritsch
P. Girard
J. Hähner
T. Heiber
R. Kilian-Kehr
M. Kinateder
D. Kügler
M. Langheinrich
P. Robinson
M. Rohs
H. Rossnagel
H. Vogt
S. Wittmann

Sponsoring Institutions

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Saarbrücken, Germany
Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany

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