Lecture Notes in Computer Science

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
   Lancaster University, UK
Takeo Kanade
   Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
   University of Surrey, Guildford, UK
Jon M. Kleinberg
   Cornell University, Ithaca, NY, USA
Friedemann Mattern
   ETH Zurich, Switzerland
John C. Mitchell
   Stanford University, CA, USA
Moni Naor
   Weizmann Institute of Science, Rehovot, Israel
Oscar Nierstrasz
   University of Bern, Switzerland
C. Pandu Rangan
   Indian Institute of Technology, Madras, India
Bernhard Steffen
   University of Dortmund, Germany
Madhu Sudan
   Massachusetts Institute of Technology, MA, USA
Demetri Terzopoulos
   New York University, NY, USA
Doug Tygar
   University of California, Berkeley, CA, USA
Moshe Y. Vardi
   Rice University, Houston, TX, USA
Gerhard Weikum
   Max-Planck Institute of Computer Science, Saarbruecken, Germany
Preface

This volume contains the papers presented at the 2nd International Conference on Security in Pervasive Computing (SPC 2005) held April 6–8, 2005 in Boppard, Germany. The objective of this second conference was to develop new security concepts for complex application scenarios based on systems like handhelds, phones, smartcards, RFID-chips and smart labels hand in hand with the emerging technology of ubiquitous and pervasive computing. In particular the conference focused on methods and technologies concerning the identification of risks, the definition of security policies, and the development of security and privacy measures, especially cryptographic protocols that are related to specific aspects of ubiquitous and pervasive computing like mobility, location-based services, ad hoc networking, resource allocation/restriction, invisibility, and secure hardware/software platforms.

We received 48 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 efficiency in processing the work and also for the quality of their reviews and discussions. Finally the Program Committee decided to accept 14 long papers and 3 short papers.

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 the local organization of the conference in Boppard. SPC 2005 was hosted by the Bundesakademie für öffentliche Verwaltung of the Federal Ministry of the Interior, and was sponsored by the DFKI and BSI.

April 2005  Dieter Hutter and Markus Ullmann
Organization

SPC 2005 was organized by the German Research Center for Artificial Intelligence (DFKI GmbH) in Saarbrücken and the German Federal Office for Information Security (BSI) in Bonn.

Executive Committee

Program Co-chairs
- Dieter Hutter (DFKI GmbH, Germany)
- Markus Ullmann (BSI, Germany)

Local Arrangements
- Hans-Peter Wagner (BSI, Germany)

Program Committee

N. Asokan, Nokia Research
Michael Beigl, University of Karlsruhe, Germany
Sonja Buchegger, EPFL-IC-LCA, Switzerland
Dieter Hutter, DFKI Saarbrücken, Germany
Ari Juels, RSA Lab, USA
Paul Karger, IBM Center Watson Research T.J., USA
Dennis Kuegler, BSI, Bonn, Germany
Catherine Meadows, Naval Research Lab, USA
Takashi Moriyasu, Hitachi Ltd., Japan
Guenter Müller, University of Freiburg, Germany
Panos Papadimitratos, Cornell University, USA
Joachim Posegga, University of Hamburg, Germany
Yves Roudier, Institut Eurecom, France
Andrei Serjantov, The Free Haven Project, UK
Frank Stajano, Cambridge University, UK
Werner Stephan, DFKI Saarbrücken, Germany
Seiji Tomita, NTT Information Platform Laboratories, Japan
Markus Ullmann, BSI, Bonn, Germany

Invited Speakers

Lorenz M. Hilty, Swiss Federal Lab for Material Testing
Panos Papadimitratos, Cornell University, USA
Dennis Kuegler, BSI, Bonn, Germany
Frederic Thiesse, University of St. Gallen
Claudia Eckert, TH Darmstadt and FhG Darmstadt
Additional Referees

D. Balfanz  A. Hohl  G. Rock
L. Buttyan  H. Kelter  E. Rukzio
L. Cheikhrouhou  F. Koob  D. Schreckling
N. Courtois  R. Monroy  H. Schwigon
G. Durfee  A. Nonnengart  J. Seedorf
D. Forsberg  K. Nyberg  J. Suomalainen
M. Gilliot  C. Partridge  C. Wieschebrink
E. Gun Sirer  H.C. Poehls  S. Wohlgemuth

Sponsoring Institutions

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH DFKI, Saarbrücken, Germany
Federal Office for Information Security, Germany.
# Table of Contents

## Invited Talk (Abstract)

Pervasive Computing - A Case for the Precautionary Principle?
*Lorenz M. Hilty* ........................................ 1

## Session 1: Smart Devices and Applications

TENeT: A Framework for Distributed Smartcards
*Masayuki Terada, Kensaku Mori, Kazuhiko Ishii, Sadayuki Hongo, Tomonori Usaka, Noboru Koshizuka, Ken Sakamura* ................................. 3

P2P Digital Value Fair Trading System Using Smart Cards
*Masayuki Hanadate, Masayuki Terada, Shinji Nagao, Toshiyuki Miyazawa, Yukiko Yosuke, Seiji Tomita, Ko Fujimura* ................................. 18

“Devices Are People Too” Using Process Patterns to Elicit Security Requirements in Novel Domains: A Ubiquitous Healthcare Example
*Yang Liu, John A. Clark, Susan Stepney* ................................. 31

## Invited Talk (Abstract)

Securing Ad Hoc Networks
*Panos Papadimitratos* ........................................ 46

## Session 2: Short Paper Session

Secure Identity Management for Pseudo-Anonymous Service Access
*Michael Hitchens, Judy Kay, Bob Kummerfeld, Ajay Brar* ................................. 48

Security Issues for Pervasive Personalized Communication Systems
*Bertin Klein, Tristan Miller, Sandra Zilles* ................................. 56

Safeguards in a World of Ambient Intelligence
*Michael Friedewald* ........................................ 63
Session 3: Authentication (I)

Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment
Keunwoo Rhee, Jin Kwak, Seungjoo Kim, Dongho Won .......................... 70

Invited Talk (Abstract)

Security Concept of the EU-Passport
Dennis Kügler ................................................................. 85

Session 4: Authentication (II)

Efficient Cooperative Signatures: A Novel Authentication Scheme for Sensor Networks
Stefaan Seys, Bart Preneel .................................................. 86

Ephemeral Pairing on Anonymous Networks
Jaap-Henk Hoepman ....................................................... 101

Invited Talk (Abstract)

EPC Technology
Christian Floerkemeier, Frederic Thiesse ................................. 117

Session 5: Authentication (III)

Exploiting Empirical Engagement in Authentication Protocol Design
Sadie Creese, Michael Goldsmith, Richard Harrison, Bill Roscoe,
Paul Whittaker, Irfan Zakiuddin ......................................... 119

Supporting Dynamically Changing Authorizations in Pervasive Communication Systems
Adam J. Lee, Jodie P. Boyer, Chris Drexelius, Prasad Naldurg,
Raquel L. Hill, Roy H. Campbell ........................................ 134

Look Who’s Talking - Authenticating Service Access Points
Adolf Hohl, Lutz Lowis, Alf Zugenmaier ................................ 151

Invited Talk (Abstract)

Security Issues of Mobile Devices
Claudia Eckert ................................................................. 163
## Session 6: Privacy and Anonymity

Privacy for Profitable Location Based Services  
*Tobias Kölisch, Lothar Fritsch, Markulf Kohlweiss, Dogan Kesdogan*  
   ................................................................. 164

On the Anonymity of Periodic Location Samples  
*Marco Gruteser, Baik Hoh*  
   ........................................................................... 179

## Session 7: Access Control and Information Flow

A Theorem Proving Approach to Analysis of Secure Information Flow  
*Ádám Darvas, Reiner Hähnle, David Sands*  
   ............................................................................. 193

An Efficient Access Control Model for Mobile Ad-Hoc Communities  
*Sye Loong Keoh, Emil Lupu*  
   ............................................................................. 210

TrustAC: Trust-Based Access Control for Pervasive Devices  
*Florina Almenárez, Andrés Marín, Celeste Campo, Carlos García R.*  
   ............................................................................. 225

## Author Index

............................................................................. 239