

*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

*University of California, Los Angeles, CA, 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*

John A. Clark Richard F. Paige  
Fiona A.C. Polack Phillip J. Brooke (Eds.)

# Security in Pervasive Computing

Third International Conference, SPC 2006  
York, UK, April 18-21, 2006  
Proceedings

Volume Editors

John A. Clark  
Richard F. Paige  
Fiona A.C. Polack  
University of York  
Department of Computer Science  
Heslington, York, YO10 5DD, UK  
E-mail: {jac.paige,fiona}@cs.york.ac.uk

Phillip J. Brooke  
University of Teesside  
School of Computing  
Middlesbrough, TS1 3BA, UK  
E-mail: p.j.brooke@tees.ac.uk

Library of Congress Control Number: 2006923045

CR Subject Classification (1998): C.2, D.2, D.4.6, H.5, K.4.1, K.4.4, K.6.5, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN            0302-9743  
ISBN-10        3-540-33376-2 Springer Berlin Heidelberg New York  
ISBN-13        978-3-540-33376-0 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2006  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper    SPIN: 11734666    06/3142    5 4 3 2 1 0

# Preface

This volume contains the papers presented at the Third International Conference on Security in Pervasive Computing (SPC 2006), held April 19–21, 2006 in York, UK. The conference focused on methods, tools, principles, and practices for assessing and achieving security in a pervasive environment. New security concepts were discussed, in domains and applications such as handheld devices, mobile phones, smartcards, RFID chips, and smart labels, as well as new, emerging technological spaces. The conference also presented work on fundamental themes such as risk identification and mitigation, security policies for pervasive environments, privacy measures (especially cryptographic protocols), and mobility and location-aware services. Submissions included work on biometrics, ambient intelligence, Web services, security requirements, and many other topics.

We received 56 submissions, and accepted 16 full papers for presentation. Each submission was reviewed by the international Programme Committee. We are grateful to the Programme Committee members, and the additional reviewers, for their timely completion of the reviewing process, and for the quality and detail of their reviews and discussion.

Our thanks go to all members of the Programme Committee for their efforts; the additional reviewers; the authors, for submitting their papers; the keynote speaker, Frank Stajano; the invited speaker, Howard Chivers; and the Department of Computer Science, University of York, for supporting the event.

April 2006

John A. Clark (Program Chair)  
Richard F. Paige  
Fiona A.C. Polack  
Phillip J. Brooke

# Organization

SPC 2006 was organized by the Department of Computer Science, University of York.

## Executive Committee

Program Chair	John A. Clark (Univ. of York, UK)
Organizing Co-chairs	Richard F. Paige and Fiona A.C. Polack (Univ. of York, UK)
Publicity Chair	Phillip J. Brooke (Univ. of Teesside, UK)

## Programme Committee

Anos Anastassiadis	Cyveillance, USA
N. Asokan	Nokia, Finland
Phil Brooke	Univ. of Teesside, UK
Howard Chivers	Cranfield University, UK
Stephen J. Crane	HP, UK
Sadie Creese	QinetiQ, UK
Michael Goldsmith	Formal Systems Europe, UK
Stefanos Gritzalis	Univ. of the Aegean, Greece
Jochen Haller	SAP, Germany
Dieter Hutter	DFKI, Germany
Paul Karger	IBM, USA
Dennis Kuegler	BSI, Germany
Marc Langheinrich	ETH Zurich, Switzerland
Cetin Kaya Koc	Oregon State, USA
Cathy Meadows	NRL, USA
Takashi Moriyasu	National Information Security Center, Japan
Guenter Mueller	Univ. of Freiburg, Germany
Richard Paige	Univ. of York, UK
Panos Papadimitratos	Virginia Tech, USA
Fiona Polack	Univ. of York, UK
Yves Roudier	Eurecom, France
Peter Ryan	Univ. of Newcastle, UK
Andrei Serjantov	Free Haven Project, UK
Werner Stephan	DFKI, Germany
Markus Ullman	BSI, Germany
Irfan Zakuidin	QinetiQ, UK

**Additional Referees**

F. Aivaloglou

J. Bryans

L. Gymnopoulos

C. Kalloniatis

G. Kambourakis

Y. Karabulut

F. Kerschbaum

R. Monroy

T. Peacock

P. Robinson

M. Volkamer

# Table of Contents

## Invited Talk

Trust Without Identification <i>Howard Chivers</i> .....	1
---	---

## Protocols

Constant-Round Password-Based Group Key Generation for Multi-layer Ad-Hoc Networks <i>Jin Wook Byun, Su-Mi Lee, Dong Hoon Lee, Dowon Hong</i> .....	3
Enabling Secure Discovery in a Pervasive Environment <i>Slim Trabelsi, Jean-Christophe Pazzaglia, Yves Roudier</i> .....	18
Forward Secure Communication in Wireless Sensor Networks <i>Sjouke Mauw, Ivo van Vessem, Bert Bos</i> .....	32

## Mechanisms

Low Rate DoS Attack to Monoprocess Servers <i>Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, Pedro García-Teodoro</i> .....	43
Delegating Secure Logging in Pervasive Computing Systems <i>Rafael Accorsi, Adolf Hohl</i> .....	58
Implementing Minimized Multivariate PKC on Low-Resource Embedded Systems <i>Bo-Yin Yang, Chen-Mou Cheng, Bor-Rong Chen, Jiun-Ming Chen</i> .....	73

## Integrity

Higher Dependability and Security for Mobile Applications <i>Hongxia Jin</i> .....	89
Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks <i>Alexander Becher, Zinaida Benenson, Maximillian Dornseif</i> .....	104

## Privacy and Security

The Brave New World of Ambient Intelligence: An Analysis of Scenarios Regarding Privacy, Identity and Security Issues  
*Michael Friedewald, Elena Vildjiounaite, Yves Punie, David Wright* . . . . . 119

Profiles and Context Awareness for Mobile Users – A Middleware Approach Supporting Personal Security  
*Gerald Eichler, Matthias O. Will* . . . . . 134

Privacy Sensitive Location Information Systems in Smart Buildings  
*Jodie P. Boyer, Kaijun Tan, Carl A. Gunter* . . . . . 149

Silent Cascade: Enhancing Location Privacy Without Communication QoS Degradation  
*Leping Huang, Hiroshi Yamane, Kanta Matsuura, Kaoru Sezaki* . . . . . 165

## Information Flow and Access Control

Securing Information Gateways with Derivation-Constrained Access Control  
*Urs Hengartner, Peter Steenkiste* . . . . . 181

Information Flow Control to Secure Dynamic Web Service Composition  
*Dieter Hutter, Melanie Volkamer* . . . . . 196

## Authentication

Analysing a Biometric Authentication Protocol for 3G Mobile Systems Using CSP and Rank Functions  
*Siraj A. Shaikh, Christos K. Dimitriadis* . . . . . 211

Attribute-Based Authentication Model for Dynamic Mobile Environments  
*Michael J. Covington, Manoj R. Sastry, Deepak J. Manohar* . . . . . 227

**Author Index** . . . . . 243