

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

Javier Lopez Pierangela Samarati
Josep L. Ferrer (Eds.)

Public Key Infrastructure

4th European PKI Workshop:
Theory and Practice, EuroPKI 2007
Palma de Mallorca, Spain, June 28-30, 2007
Proceedings

Volume Editors

Javier Lopez

University of Malaga, Computer Science Department, E.T.S.I. Informatica

Campus Teatinos, 29071 Malaga, Spain

E-mail: jlm@lcc.uma.es

Pierangela Samarati

Università degli Studi di Milano, Dipartimento di Tecnologie dell'Informazione

v. Bramante 65, 26013 Crema, Italy

E-mail: samarati@dti.unimi.it

Josep L. Ferrer

University of Balearic Islands, Computer Science Department

07122 Palma, Spain

E-mail: dmijfg0@uib.es

Library of Congress Control Number: 2007929479

CR Subject Classification (1998): E.3, D.4.6, C.2.0, F.2.1, H.3, H.4, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-73407-4 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-73407-9 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

© Springer-Verlag Berlin Heidelberg 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12085347 06/3180 5 4 3 2 1 0

Preface

These proceedings contain the papers accepted at the 2007 European PKI Workshop: Theory and Practice (EuroPKI 2007), held in Palma de Mallorca, Spain, during June 28–30, and hosted by the Computer Science Department of the University of Balearic Islands (UIB) with the support of the Balearic Islands Government and the Private Law Department at UIB. This year's event was the fourth event in the EuroPKI Workshops series. Previous events of the series were held in: Samos, Greece (2004); Kent, UK (2005); and Turin, Italy, (2006).

In response to the call for papers, 77 papers were submitted to this year's workshop, setting a record of the highest number of papers submitted to an EuroPKI event so far and confirming an increased interest in PKI research and in the EuroPKI event. Each paper was reviewed by three members of the Program Committee, and evaluated on the basis of its significance, novelty, technical quality and relevance to the workshop. The paper selection process was very competitive: of the papers submitted, only 21 full papers and 8 short papers were selected for presentation at the workshop and inclusion in this volume.

We would like to thank all those people who, in a different capacity, contributed to the realization of this event. Thank you to all the members of the Program Committee and to the external reviewers for their constructive and insightful comments during the review process. Thank you to the staff of Springer for their co-operation and their excellent work during the publication process. Special thanks to: the members of the Organizing Committee for their hard work in dealing with all matters related to the conference organization; to the sponsors, for their valuable support; and to the invited speakers, Bart Preneel and Gene Tsudik, for accepting our invitation to deliver a talk.

Finally, we would like to thank all the authors who submitted papers to the workshop, including those whose submissions were not selected for publication, and all the workshop attendees. We hope that you find the proceedings interesting.

June 2007

Javier Lopez
Pierangela Samarati
Josep L. Ferrer

EuroPKI 2007
Fourth European PKI Workshop:
Theory and Practice

Palma de Mallorca, Spain
28-30 June, 2007

Organized by
Computer Science Department
University of Balearic Islands
Spain

Program Co-chairs

Javier Lopez
Pierangela Samarati

University of Malaga, Spain
University of Milan, Italy

General Chair

Josep L. Ferrer

University of Balearic Islands, Spain

Workshop Chair

Llorenç Huguet

University of Balearic Islands, Spain

Program Committee

Carlisle Adams
Oscar Canovas
Sabrina De Capitani di Vimercati
David Chadwick
Marco Cremonini
Jorge Davila
Ed Dawson
Stephen Farrell
Jordi Forne
Dieter Gollmann
Stefanos Gritzalis
Dimitris Gritzalis
Socrates Katsikas
Stephen Kent
Kwangjo Kim
Chi-Sung Laih
Antonio Lioy

University of Ottawa, Canada
University of Murcia, Spain
University of Milan, Italy
University of Kent, UK
University of Milan, Italy
Polytechnic University of Madrid, Spain
Queensland University of Technology, Australia
Trinity College Dublin, Ireland
Polytechnic University of Catalonia, Spain
Hamburg University of Technology, Germany
University of the Aegean, Greece
AUEB, Greece
University of the Aegean, Greece
BBN Technologies, USA
ICU, Korea
National Cheng Kung University, Taiwan
Politecnico di Torino, Italy

Fabio Martinelli	IIT-CNR, Italy
Apol·lonia Martinez	University of Balearic Islands, Spain
Fabio Massacci	University of Trento, Italy
Stig F. Mjøl̂snes	NTNU, Norway
Jose A. Montenegro	University of Malaga, Spain
Yi Mu	University of Wollongong, Australia
Rolf Oppliger	eSecurity, Switzerland
Eiji Okamoto	University of Tsukuba, Japan
Jong Hyuk Park	Hanwha S&C Co., Korea
Guenter Pernul	University of Regensburg, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Chunming Rong	University of Stavanger, Norway
Kouichi Sakurai	Kyushu University, Japan
Damien Sauveron	University of Limoges, France
Sean Smith	Dartmouth College, USA
Julien Stern	Cryptolog, France
Jianying Zhou	Institute for Infocomm Research, Singapore
Sencun Zhu	Penn State University, USA

Organization Committee

Magdalena Payeras (Chair)	University of Balearic Islands, Spain
Cristina Alcaraz	University of Malaga, Spain
Macia Mut	University of Balearic Islands, Spain
Antonia Paniza	University of Balearic Islands, Spain
Rodrigo Roman	University of Malaga, Spain

External Reviewers

François Arnault, Giulia Boato, Pierre-François Bonnefoi, Serge Chaumette, Wolfgang Dobmeier, Stelios Dritsas, Pierre Dusart, Ludwig Fuchs, Félix J. Garcia-Clemente, Theodoulos Garefalakis, Xinyi Huang, John Iliadis, George Kambourakis, Jan Kolter, Elisavet Konstantinou, Dimitris Lekkas, Ioannis Marias, Antonio Muñoz, Gregory Neven, Sassa Otenko, Vincent Rijmen, Ayda Saidane, Rolf Schillinger, Christian Schläger, Kei Lei Shi, Marianthi Theoharidou, Bill Tsoumas, Frederik Vercauteren, Guilin Wang, Artsiom Yautsiukhin, Nicola Zannone.

Sponsors



Govern de les Illes Balears

Conselleria de d'Economia, Hisenda i Innovació
Direcció General de Recerca, Desenvolupament Tecnològic i Innovació

Table of Contents

Authorization Architectures for Privacy-Respecting Surveillance	1
<i>Ulrich Flegel and Michael Meier</i>	
Privacy-Preserving Revocation Checking with Modified CRLs	18
<i>Maithili Narasimha and Gene Tsudik</i>	
E-Passports as a Means Towards the First World-Wide Public Key Infrastructure	34
<i>Dimitrios Lekkas and Dimitris Gritzalis</i>	
An Interdomain PKI Model Based on Trust Lists	49
<i>Helena Rifà-Pous and Jordi Herrera-Joancomartí</i>	
One-More Extension of Paillier Inversion Problem and Concurrent Secure Identification	65
<i>Yan Song</i>	
An Efficient Signcryption Scheme with Key Privacy	78
<i>Chung Ki Li, Guomin Yang, Duncan S. Wong, Xiaotie Deng, and Sherman S.M. Chow</i>	
Direct Chosen-Ciphertext Secure Hierarchical ID-Based Encryption Schemes	94
<i>Jong Hwan Park and Dong Hoon Lee</i>	
Certificate-Based Signature: Security Model and Efficient Construction	110
<i>Jiguo Li, Xinyi Huang, Yi Mu, Willy Susilo, and Qianhong Wu</i>	
Time Capsule Signature: Efficient and Provably Secure Constructions	126
<i>Bessie C. Hu, Duncan S. Wong, Qiong Huang, Guomin Yang, and Xiaotie Deng</i>	
A New Variant for an Attack Against RSA Signature Verification Using Parameter Field	143
<i>Yutaka Oiwa, Kazukuni Kobara, and Hajime Watanabe</i>	
AutoPKI: A PKI Resources Discovery System	154
<i>Massimiliano Pala and Sean W. Smith</i>	
Bootstrapping a Global SSO from Network Access Control Mechanisms	170
<i>Manuel Sánchez, Gabriel López, Óscar Cánovas, and Antonio F. Gómez-Skarmeta</i>	

Anonymous k -Show Credentials	181
<i>Mohamed Layouni and Hans Vangheluwe</i>	
On Partial Anonymity in Secret Sharing	193
<i>Vanesa Daza and Josep Domingo-Ferrer</i>	
Anonymous Identification and Designated-Verifiers Signatures from Insecure Batch Verification	203
<i>Sherman S.M. Chow and Duncan S. Wong</i>	
OpenHSM: An Open Key Life Cycle Protocol for Public Key Infrastructure's Hardware Security Modules	220
<i>Jean Everson Martina, Tulio Cicero Salvaro de Souza, and Ricardo Felipe Custodio</i>	
Two Worlds, One Smart Card: An Integrated Solution for Physical Access and Logical Security Using PKI on a Single Smart Card	236
<i>Jaap-Henk Hoepman and Geert Kleinhuis</i>	
On the Robustness of Applications Based on the SSL and TLS Security Protocols	248
<i>Diana Berbecaru and Antonio Lioy</i>	
Using WebDAV for Improved Certificate Revocation and Publication . . .	265
<i>David W. Chadwick and Sean Anthony</i>	
Reducing the Computational Cost of Certification Path Validation in Mobile Payment	280
<i>Cristina Satizábal, Rafael Martínez-Peláez, Jordi Forné, and Francisco Rico-Novella</i>	
Security-by-Contract: Toward a Semantics for Digital Signatures on Mobile Code	297
<i>N. Dragoni, F. Massacci, K. Naliuka, and I. Siahaan</i>	
Applicability of Public Key Infrastructures in Wireless Sensor Networks	313
<i>Rodrigo Roman and Cristina Alcaraz</i>	
Spatial-Temporal Certification Framework and Extension of X.509 Attribute Certificate Framework and SAML Standard to Support Spatial-Temporal Certificates	321
<i>Ana Isabel González-Tablas Ferreres, Benjamín Ramos Álvarez, and Arturo Ribagorda Garnacho</i>	
Electronic Payment Scheme Using Identity-Based Cryptography	330
<i>Son Thanh Nguyen and Chunming Rong</i>	
Undeniable Mobile Billing Schemes	338
<i>Shiqun Li, Guilin Wang, Jianying Zhou, and Kefei Chen</i>	

Universally Composable Signcryption	346
<i>Kristian Gjøsteen and Lillian Kråkmo</i>	
Chord-PKI: Embedding a Public Key Infrastructure into the Chord Overlay Network	354
<i>Agapios Avramidis, Panayiotis Kotzanikolaou, and Christos Douligeris</i>	
Privacy Protection in Location-Based Services Through a Public-Key Privacy Homomorphism	362
<i>Agusti Solanas and Antoni Martínez-Ballesté</i>	
A Critical View on RFC 3647	369
<i>Klaus Schmeh</i>	
Author Index	375