Lecture Notes in Computer Science 4582

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

Editorial Board

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

Springer

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

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	University of Malaga, Spain
Pierangela Samarati	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	University of Ottawa, Canada
Oscar Canovas	University of Murcia, Spain
Sabrina De Capitani di Vimercati	University of Milan, Italy
David Chadwick	University of Kent, UK
Marco Cremonini	University of Milan, Italy
Jorge Davila	Polytechnic University of Madrid, Spain
Ed Dawson	Queensland University of Technology, Australia
Stephen Farrell	Trinity College Dublin, Ireland
Jordi Forne	Polytechnic University of Catalonia , Spain
Dieter Gollmann	Hamburg University of Technology, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Dimitris Gritzalis	AUEB, Greece
Socrates Katsikas	University of the Aegean, Greece
Stephen Kent	BBN Technologies, USA
Kwangjo Kim	ICU, Korea
Chi-Sung Laih	National Cheng Kung University, Taiwan
Antonio Lioy	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. Mjølsnes	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 Stanvanger, 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