Lecture Notes in Computer Science 7163

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

Svetla Petkova-Nikova Andreas Pashalidis
Günther Pernul (Eds.)

Public Key Infrastructures, Services, and Applications

8th European Workshop, EuroPKI 2011
Leuven, Belgium, September 15-16, 2011
Revised Selected Papers

Springer

Volume Editors

Svetla Petkova-Nikova
University of Twente, the Netherlands
and Katholieke Universiteit Leuven ESAT-COSIC
Kasteelpark Arenberg 10
3001 Leuven-Heverlee, Belgium
E-mail: svetla.nikova@esat.kuleuven.be

Andreas Pashalidis
Katholieke Universiteit Leuven ESAT/SCD (COSIC)
Kasteelpark Arenberg 10
3001 Leuven-Heverlee, Belgium
andreas.pashalidis@esat.kuleuven.be

Günther Pernul
University of Regensburg
Department of Information Systems
Universitätsstraße 31
93053 Regensburg, Germany
E-mail: guenther.pernul@wiwi.uni-regensburg.de

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-29803-5 e-ISBN 978-3-642-29804-2
DOI 10.1007/978-3-642-29804-2
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012937469

CR Subject Classification (1998): K.6.5, C.2, E.3, D.4.6, J.1, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

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

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This book contains the proceedings of the 8th European Workshop on Public Key Infrastructures, Services, and Applications (EuroPKI 2011), held in Leuven, Belgium, during September 15–16, 2011.

The aim of the EuroPKI workshop series is to stimulate and promote international research and collaboration on all aspects of public key services, applications and infrastructures, including innovative applications of public key cryptography. The workshop is intended for security researchers and practitioners as well as for participants from industry that are active in the field of public key services, applications, infrastructures and, in general, information security. This year's workshop was co-located with the 16th European Symposium on Research in Computer Security (ESORICS) and took place at the Katholieke Universiteit Leuven. Previous events were held in Samos (EuroPKI 2004), Kent (EuroPKI 2005), Turin (EuroPKI 2006), Mallorca (EuroPKI 2007), Trondheim (EuroPKI 2008), Pisa (EuroPKI 2009), and Athens (EuroPKI 2010).

This volume holds ten refereed papers and the presentation papers by the invited speakers, Chris J. Mitchell, Peter Gutmann, and Olivier Pereira. In response to the EuroPKI 2011 call for papers, 27 submissions were received. Each submission was subjected to a thorough review by at least three Program Committee members and external reviewers, resulting in a stringent selection and careful revision of the accepted papers. After the workshop, authors revised their papers again and provided improved versions for inclusion in this volume.

We wish to thank everyone who contributed toward the success of the workshop: the authors of submitted contributions, the Program Chairs and the Program Committee for their efforts in reviewing and discussing the submission under tight time constraints. Many thanks also to Christian Broser for his publicity work and to Michael Weber for collecting the papers and his help editing this book. We are grateful to our sponsor LSEC, and to Ulrich Seldeslachts for organizing a special session with speakers from the security industry during the event, as well as for moderating the lively discussions between workshop attendees and speakers. Special thanks go to the local organizers including, among many others, Saartje Verheyen for dealing with a host of administrative and bookkeeping issues; Sebastiaan Indesteege for his help with the EuroPKI 2011 website; Roel Peeters for managing electronic workshop registrations and payments; and Bart Preneel for his general support.

September 2011

Svetla Nikova
Andreas Pashalidis
Günther Pernul

Organization

General Chair

Andreas Pashalidis	Katholieke Universiteit Leuven, Belgium

Program Committee Chairs

Svetla Nikova	Katholieke Universiteit Leuven, Belgium and University of Twente, The Netherlands
Günther Pernul	University of Regensburg, Germany

Publicity Chair

Christian Broser	University of Regensburg, Germany

International Program Committee

F. Bao	Institute for Infocomm Research, Singapore
L. Batina	Radboud University Nijmegen, Katholieke Universiteit Leuven, The Netherlands, Belgium
D. Chadwick	Kent University, UK
S. Chow	University of Waterloo, Canada
M. Cremonini	University of Milan, Italy
P. D'Arco	University of Salerno, Italy
S. De Capitani di Vimercati	University of Milan, Italy
A.W. Dent	Royal Holloway, University of London, UK
R. Di Pietro	University of Rome III, Italy
S. Furnell	University of Plymouth, UK
J. Gonzalez-Nieto	Queensland University of Technology, Australia
P. Gutmann	University of Auckland, New Zealand
S. Katsikas	University of Piraeus, Greece
S. Kent	BBN Technologies, USA
D. Kesdogan	University Siegen, Germany
E. Konstantinou	University of the Aegean, Greece
K. Kursawe	Radboud University Nijmegen, The Netherlands

C. Lambrinoudakis	University of Piraeus, Greece
H. Leitold	TU Graz, Austria
J. Lopez	University of Malaga, Spain
F. Martinelli	National Research Council, Italy
C. Meadows	NRL, USA
S. Mjølsnes	Norwegian University of Science and Technology, Norway
Y. Mu	University of Wollongong, Australia
R. Oppliger	eSECURITY Technologies, Switzerland
M. Pala	Dartmouth College, USA
O. Pereira	Universite Catholique de Louvain, Belgium
B. Preneel	Katholieke Universiteit Leuven, Belgium
S. Radomirovic	University of Luxembourg, Luxembourg
P. Samarati	Università degli Studi di Milano, Italy
S. Seys	Katholieke Universiteit Leuven, Belgium
S. Smith	Dartmouth College, USA

Subreviewers

Au, Man Ho	Fuchs, Ludwig	Lazouski, Aliaksandr
Chen, Xihui	Gmelch, Oliver	Netter, Michael
Chu, Cheng-Kang	Han, Jinguang	Pham, Vinh
Dietrich, Kurt	Ibraimi, Luan	Zefferer, Thomas
Fritsch, Christoph	Krautsevich, Leanid	

Table of Contents

PKI Applications

Secure Applications