Lecture Notes in Computer Science 7868

Sabrina De Capitani di Vimercati
Chris Mitchell (Eds.)

Public Key Infrastructures, Services and Applications

9th European Workshop, EuroPKI 2012
Pisa, Italy, September 13-14, 2012
Revised Selected Papers

Springer

Volume Editors

Sabrina De Capitani di Vimercati
Università degli Studi di Milano
Dipartimento de Informatica
26013 Crema, Italy
E-mail: sabrina.decapitani@unimi.it

Chris Mitchell
University of London, Royal Holloway
Egham, Surrey TW20 0EX, UK
E-mail: c.mitchell@rhul.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-40011-7 e-ISBN 978-3-642-40012-4
DOI 10.1007/978-3-642-40012-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013944638

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

These proceedings contain the papers selected for presentation at the 9th European PKI Workshop: Research and Applications, held September 13–14, 2012, in conjunction with ESORICS 2012, in Pisa, Italy.

In response to the call for papers, 30 papers were submitted to the workshop. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the Program committee. Reviewing was double-blind meaning that the Program committee was not able to see the names and affiliations of the authors, and the authors were not told which committee members reviewed which papers. The Program Committee meeting was held electronically, with intensive discussion over a period of two weeks. Of the papers submitted, 12 were selected for presentation at the workshop, giving an acceptance rate of 40%.

There is a long list of people who volunteered their time and energy to put together the workshop and who deserve acknowledgment. Thanks to all the members of the Program Committee, and the external reviewers, for all their hard work in evaluating and discussing papers. We would like to thank Fabio Martinelli for overall organization as General Chair of ESORICS 2012, Giovanni Livraga, for taking care of publicity and of the workshop website, Sara Foresti for collating this volume, and the invited speakers Kenny Paterson and Roberto Di Pietro. We are also very grateful to all other ESORICS 2012 organizers whose work ensured a smooth organizational process.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you find the program stimulating.

Sabrina De Capitani di Vimercati
Chris Mitchell

Organization

General Chair

Fabio Martinelli	National Research Council - CNR, Italy

Program Chairs

Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Chris Mitchell	Royal Holloway, University of London, UK

Publicity Chair

Giovanni Livraga	Università degli Studi di Milano, Italy

Program Committee

Lejla Batina	Radboud University Nijmegen, The Netherlands
Carlos Blanco Bueno	University of Cantabria, Spain
David Chadwick	University of Kent, UK
Sherman S.M. Chow	University of Waterloo, Canada
Paolo D'Arco	University of Salerno, Italy
Bao Feng	Institute for Infocomm Research, Singapore
Simone Fischer-Huebner	Karlstad University, Sweden
Sara Foresti	Università degli Studi di Milano, Italy
Steven Furnell	Plymouth University, UK
Peter Gutmann	University of Auckland, New Zealand
Ravi Jhawar	Università degli Studi di Milano, Italy
Sokratis Katsikas	University of Piraeus, Greece
Dogan Kesdogan	University of Siegen, Germany
Elisavet Konstantinou	University of the Aegean, Greece
Costas Lambrinoudakis	University of Piraeus, Greece
Herbert Leitold	A-SIT, Austria
Javier Lopez	University of Malaga, Spain
Fabio Martinelli	National Research Council - CNR, Italy
Catherine Meadows	NRL, USA
Stig Mjølsnes	NTNU, Norway
Yi Mu	University of Wollongong, Australia
Shishir Nagaraja	University of Birmingham, UK

Svetla Nikova	Katholieke Universiteit Leuven, Belgium
Rolf Oppliger	eSECURITY Technologies, Switzerland
Massimiliano Pala	Polytechnic Institute, USA
Stefano Paraboschi	Università degli Studi di Bergamo, Italy
Andreas Pashalidis	K.U. Leuven, Belgium
Olivier Pereira	Universite Catholique de Louvain, Belgium
Günter Pernul	Universität Regensburg, Germany
Sasa Radomirovic	University of Luxembourg, Luxembourg
Pierangela Samarati	Università degli Studi di Milano, Italy
Sean Smith	Dartmouth College, USA

External Reviewers

Au, Man Ho
Coisel, Iwen
Drogkaris, Prokopios
Fan, Junfeng
Feltz, Michele
Fischer, Lars
Hassan, Sabri
Heupel, Marcel
Karatas, Fatih
Krautsevich, Leanid
Netter, Michael
Peters, Thomas
Rea, Scott
Riesner, Moritz
Seys, Stefaan
Slamanig, Daniel
Stengel, Ingo
Vercauteren, Frederik
Vrakas, Nikos
Zhao, Jianjie

Table of Contents

Cryptographic Schemas and Protocols

Public Key Infrastructure

Wireless Authentication and Revocation

Certificate and Trusted Computing

Digital Signatures