Lecture Notes in Computer Science 5057

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

Stig F. Mjølsnes Sjouke Mauw
Sokratis K. Katsikas (Eds.)

Public Key Infrastructure

5th European PKI Workshop:
Theory and Practice, EuroPKI 2008
Trondheim, Norway, June 16-17, 2008
Proceedings

Springer

Volume Editors

Stig F. Mjølsnes
Norwegian University of Science & Technology (NTNU)
Department of Telematics
7491 Trondheim, Norway
E-mail: sfm@item.ntnu.no

Sjouke Mauw
Université du Luxembourg
Faculté des Sciences, de la Technologie et de la Communication (FSTC)
6 rue Richard Coudenhove-Kalergi, 1359 Luxembourg-Kirchberg, Luxembourg
E-mail: sjouke.mauw@uni.lu

Sokratis K. Katsikas
University of Piraeus
Department of Technology Education & Digital Systems
150 Androutsou St., 18532 Piraeus, Greece
E-mail: ska@unipi.gr

Library of Congress Control Number: 2008928842

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 3-540-69484-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-69484-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12320028 06/3180 5 4 3 2 1 0

Preface

This book contains the proceedings of the 5th European Public Key Infrastructure Workshop: Theory and Practice, EuroPKI 2008, which was held on the NTNU campus Gløshaugen in Trondheim, Norway, in June 2008.

The EuroPKI workshop series focuses on all research and practice aspects of public key infrastructures, services and applications, and welcomes original research papers and excellent survey contributions from academia, government, and industry.

Simply put, public keys are easier to distribute than secret keys. Nevertheless, constructing effective, practical, secure and low cost means for assuring authenticity and validity of public keys used in large-scale networked services remains both a technological and organizational challenge. In a nutshell, this is the PKI problem, and the papers presented herein propose new solutions and insight for these questions.

This volume holds 16 refereed papers including the presentation paper by the invited speaker P. Landrock. In response to the EuroPKI 2008 call for papers, a total of 37 paper proposals were received. All submissions underwent a thorough blind review by at least three PC members, resulting in a careful selection and revision of the accepted papers. The authors came from 10 countries: Belgium, Brazil, Canada, Finland, Germany, Japan, Malaysia, Norway, Spain, and the USA. The accepted papers were organized into the topical sessions: Invited Talk, Certificates, Authentication, Practice, Signatures, Analysis, and Networks.

The use and exploitation of large-scale public key infrastructures have arrived at a slower tempo and perhaps in other directions than originally envisioned a decade ago. A case in point, only 2 out of 16 authors in this workshop found it convenient to provide a digital signature on the copyright transfer form for the submitted paper. So we are not there yet!

We thank all the people who contributed to this workshop: the authors, the invited speaker, the members of the Program Committee, the members of the Organization Committee, the staff at Springer, the sponsors for their support, and finally all the workshop participants. They all made this workshop successful.

June 2008

Stig F. Mjølsnes
Sjouke Mauw
Sokratis Katsikas

Organization

EuroPKI 2008 was hosted by NTNU.

Chairs

General Chair	Stig F. Mjølsnes, Norwegian University of Science and Technology (Norway)
Program Chairs	Sjouke Mauw, University of Luxembourg (Luxembourg)
	Sokratis Katsikas, University of Piraeus (Greece)
Organizing Chair	Martin Eian, Norwegian University of Science and Technology (Norway)

Program Committee

I. Agudo Ruiz, University of Malaga, Spain
S. De Capitani di Vimercati, University of Milan, Italy
D. Chadwick, Kent University, UK
C. Cremers, ETHZ, Switzerland
M. Cremonini, University of Milan, Italy
E. Dawson, Queensland University of Technology, Australia
S. Farrell, Trinity College Dublin, Ireland
S. Furnell, University of Plymouth, UK
K. Gjøsteen, Norwegian University of Science and Technology, Norway
D. Gollmann, Technical University Hamburg, Germany
S. Gritzalis, University of the Aegean, Greece
D. Gritzalis, Athens University of Economics and Business, Greece
J. Guajardo, Philips Research Europe, The Netherlands
P. Gutmann, University of Auckland, New Zealand
A. Jøsang, Queensland University of Technology, Australia
S. Kent, BBN Technologies, USA
D. Kesdogan, Siegen University, Germany
E. Konstantinou, University of the Aegean, Greece
D. Lekkas, University of the Aegean, Greece
A. Lioy, Politecnico di Torino, Italy
J. Lopez, University of Malaga, Spain
F. Martinelli, CNR, Italy
F. Massacci, University of Trento, Italy
C. Meadows, NRL, USA
C. Mitchell, Royal Holloway College, UK

S. Mjølsnes, Norwegian University of Science and Technology, Norway
Y. Mu, University of Wollongong, Australia
E. Okamoto, Tsukuba University, Japan
R. Oppliger, eSECURITY Technologies, Switzerland
T. Pedersen, Cryptomathic, Denmark
G. Pernul, University of Regensburg, Germany
D. Polemi, University of Piraeus, Greece
B. Preneel, Katholieke University Leuven, Belgium
S. Radomirović, University of Luxembourg, Luxembourg
M. Roe, Microsoft, UK
C. Rong, University of Stavanger, Norway
K. Sakurai, Kyushu University, Japan
R. Sandhu, University of Texas San Antonio, USA
B. Schoenmakers, Eindhoven University of Technology, The Netherlands
S. Smith, Dartmouth College, USA
Y. Stamatiou, University of Ioannina, Greece
G. Tsudik, University of California Irvine, USA
J. Zhou, Institute for Infocomm Research, Singapore
S. Zhu, Penn State University, USA
C. Xenakis, University of Piraeus, Greece

Organization Committee

Jorunn Sommervold, Peter Herrmann, NTNU
Ingrid Melve, Torgrim Lauritsen, UNINETT

Sponsoring Institutions

- Department of Telematics, NTNU
- Faculty of Information Technology, Mathematics and Electrical Engineering, NTNU
- UNINETT
- NISNET (Information Security Research Network Project supported by The Research Council of Norway)

Table of Contents

Signatures

Analysis

Networks