Lecture Notes in Computer Science 3093

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

Editorial Board

Sokratis K. Katsikas Stefanos Gritzalis
Javier Lopez (Eds.)

Public Key Infrastructure

First European PKI Workshop:
Research and Applications, EuroPKI 2004
Samos Island, Greece, June 25-26, 2004
Proceedings

Springer

Volume Editors

Sokratis K. Katsikas
University of the Aegean
Rector's Office, Administration Building
University Hill, GR-81100 Mytilene, Greece
E-mail: ska@aegean.gr

Stefanos Gritzalis
University of the Aegean
Department of Information and Communication Systems Engineering
Laboratory of Information and Communication Systems Security
Karlovassi, GR-83200 Samos, Greece
E-mail: sgritz@aegean.gr

Javier Lopez
University of Malaga
Computer Science Department, E.T.S. Ingeniería Informática
Campus de Teatinos, Spain
E-mail: jlm@lcc.uma.es

Library of Congress Control Number: 2004107465

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

ISSN 0302-9743
ISBN 3-540-22216-2 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 11012214 06/3142 5 4 3 2 1 0

Preface

There is no doubt that the Internet is affecting every aspect of our lives; the most significant changes are occurring in private and public sector organizations that are transforming their conventional operating models to Internet-based service models, known as eBusiness, eCommerce and eGovernment. Companies, institutions and organizations, irrespective of their size, are nowadays utilizing the Internet for communicating with their customers, suppliers and partners; for facilitating the interconnection of their employees and branches; for connecting to their back-end data systems and for performing commercial transactions. In such an environment, where almost every organization relies heavily on information and communications technologies, new dependencies and risks arise. *Public Key Infrastructure (PKI)* is probably one of the most important items in the arsenal of security measures that can be brought to bear against the aforementioned growing risks and threats.

PKI research has been active for more than 26 years. In 1978 R.L. Rivest, A. Shamir and L. Adleman published what is now commonly called the RSA cryptosystem (*Communications of the ACM,* Vol.21, No.2, pp.120–128, 1978), one of the most significant discoveries in the history of cryptography. Since the mathematical foundation of RSA rests on the intractability of factoring large composite integers, in the same year, R. Merkle demonstrated that certain computational puzzles could also be used in constructing public key cryptography (*Communications of the ACM,* Vol.21, No.4, pp.194–299, 1978).

As the years passed by, several countries started developing their PKI. Inevitably, several practical problems were identified. Although adhering to international standards, such as ITU, ISO, IETF and PKCS, different PKI systems (national and/or international) could not connect to one another. Subsequently, a number of organizations were formed to promote and support the interoperability of different PKIs between certain countries. Indicative examples of such organizations today include the *PKI Forum,* the *EESSI – European Electronic Signature Standardization Initiative* and the *Asia PKI Forum*.

To foster and stimulate these discussions in a research environment, the *International Workshops for Asian PKI (IWAP)* and the *US PKI Research Workshops* have been held annually since 2001 (IWAP 2001 in Korea, IWAP 2002 in Taiwan, IWAP 2004 in Japan) and since 2002 (the annual US PKI Research Workshops, hosted by the NIST) respectively. Their goal is to provide a framework for both theoreticians and practitioners to share their experience and research outcomes concerning good practices in applying PKI and related supporting technologies, together with prudent assessment and comparison of the technologies.

The first *European PKI Workshop: Research and Applications (EuroPKI 2004)* initiated a series of corresponding workshop activities in Europe. The EuroPKI 2004 workshop was held on 25–26 June 2004, on Samos Island, Greece, and was hosted by the University of the Aegean, Department of Information and Communication Systems Engineering, Laboratory of Information and Communication Systems Security (*Info-Sec-Lab*, www.icsd.aegean.gr/Info-Sec-Lab).

In response to the EuroPKI 2004 call for papers, 73 papers were submitted, whose authors came from 25 countries. Each paper was reviewed by three members of the Program Committee, on the basis of the significance, novelty, technical quality and PKI relevance of the work reported therein. At the end of the reviewing process, only 25 papers were selected for presentation, whose authors came from 13 countries, resulting in an acceptance rate of 34%. This volume contains these papers as well as 5 additional short papers.

We would like to thank all the members of the Program Committee, as well as the external reviewers, for their constructive and insightful comments during the review process. Moreover, we would like to express our gratitude to the members of the Organizing Committee for their continuous and valuable support. We also wish to express our thanks to Alfred Hofmann and his colleagues from Springer-Verlag, for their co-operation and their excellent work during the publication process. Finally, we would like to thank all the people who submitted their papers to the workshop, including those whose submissions were not selected for publication, and all the delegates from around the world who attended the first *European PKI Workshop*. Without their support the workshop would not have been possible.

June 2004

Sokratis K. Katsikas
Stefanos Gritzalis
Javier Lopez

EuroPKI'2004 Workshop Committee

General Chairman

Sokratis K. Katsikas	University of the Aegean, Greece

Program Committee Co-Chairmen

Stefanos Gritzalis	University of the Aegean, Greece
Javier Lopez	University of Malaga, Spain

International Program Committee

Carlisle Adams	University of Ottawa, Canada
Giampaolo Bella	University of Catania, Italy
Ahto Buldas	Tallinn Technical University, Estonia
Mike Burmester	Florida State University, USA
Luke O'Connor	IBM, Switzerland
Sabrina De Capitani di Vimercati	University of Milan, Italy
Vassilios Chryssikopoulos	Ionian University, Greece
Ed Dawson	Queensland University of Technology, Australia
Yves Deswarte	LAAS-CNRS, France
Stephen Farrell	Trinity College Dublin, Ireland
Simon Foley	University College Corke, Ireland
Jordi Forne	Polytechnic University of Catalonia, Spain
Steven Furnell	University of Plymouth, UK
Dieter Gollmann	TU Hamburg-Harburg, Germany
Antonio Gomez-Skarmeta	University of Murcia, Spain
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Hideki Imai	University of Tokio, Japan
Sushil Jajodia	George Mason University, USA
Kwangjo Kim	Information and Communications University, Korea
Spyros Kokolakis	University of the Aegean, Greece
Constantinos Lambrinoudakis	University of the Aegean, Greece
Dimitris Lekkas	University of the Aegean, Greece
Peter Lipp	Technical University of Graz, Austria
Jose A. Mañas	Polytechnic University of Madrid, Spain
Catherine Meadows	NRL, USA

Chris Mitchell	RHBNC, University of London, UK
Refik Molva	Eurécom, France
Eiji Okamoto	University of Tsukuba, Japan
Rolf Oppliger	eSecurity, Switzerland
George Pangalos	Aristotelean University of Thessaloniki, Greece
Ahmed Patel	University College Dublin, Ireland
Guenther Pernul	University of Regensburg, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Gerald Quirchmayr	University of South Australia, Australia
Jean-Jacques Quisquater	UCL, Belgium
Peter Ryan	University of Newcastle, UK
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	University of Milan, Italy
Sean Smith	Dartmouth College, USA
Diomidis Spinellis	Athens University of Economics and Business, Greece
Julien P. Stern	Cryptolog, France
Michael Szydlo	RSA Security Inc., USA
Moti Yung	Columbia University, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

George Aggelis	University of the Aegean, Greece
Carlos Aguilar	LAAS-CNRS, France
Walid Bagga	Institut Eurecom, France
Thodoris Balopoulos	University of the Aegean, Greece
Phil Brooke	University of Plymouth, UK
Jeremy Bryans	University of Newcastle-upon-Tyne, UK
Oscar Canovas	University of Murcia, Spain
Shiping Chen	George Mason University, USA
Lazaros Gymnopoulos	University of the Aegean, Greece
DongGuk Han	Kyushu University, Japan
John Iliadis	University of the Aegean, Greece
Kenji Imamoto	Kyushu University, Japan
George Kambourakis	University of the Aegean, Greece
Satoshi Koga	Kyushu University, Japan
Gregorio Martinez	University of Murcia, Spain
Gabriel López Millán	University of Murcia, Spain
Lilian Mitrou	University of the Aegean, Greece
Björn Muschall	University of Regensburg, Germany
Melek Onen	Institut Eurecom, France

Akira Otsuka	Information Technology Promotion Agency, Japan
Thea Peacock	University of Newcastle-upon-Tyne, UK
Josep Pegueroles	Technical University of Catalonia, Spain
Agapios Platis	University of the Aegean, Greece
Fabien Pouget	Institut Eurecom, France
Torsten Priebe	University of Regensburg, Germany
Thomas Quillinan	University College Corke, Ireland
Junji Shikata	Yokohama National University, Japan
BHan Shin	Tokyo University, Japan
Seong Han Shin	Tokyo University, Japan
Vasileios Vlachos	Athens University of Economics and Business, Greece
Chao Yao	George Mason University, USA
Alec Yasinsac	Florida State University, USA
Rui Zhang	Tokyo University, Japan
Sencun Zhu	George Mason University, USA

Table of Contents