

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

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
ISBN 978-3-642-40011-7
DOI 10.1007/978-3-642-40012-4
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-40012-4

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

© Springer-Verlag Berlin Heidelberg 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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
Chris Mitchell

Università degli Studi di Milano, Italy

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

Table of Contents

Cryptographic Schemas and Protocols

Analysis of Lattice Reduction Attack against the Somewhat Homomorphic Encryption Based on Ideal Lattices	1
<i>Masaya Yasuda, Jun Yajima, Takeshi Shimoyama, and Jun Kogure</i>	
Group Key Exchange Resilient to Leakage of Ephemeral Secret Keys with Strong Contributiveness	17
<i>Cheng Chen, Yanfei Guo, and Rui Zhang</i>	
Efficient Public Key Encryption Admitting Decryption by Sender	37
<i>Puwen Wei and Yuliang Zheng</i>	

Public Key Infrastructure

How to Avoid the Breakdown of Public Key Infrastructures: Forward Secure Signatures for Certificate Authorities	53
<i>Johannes Braun, Andreas Hülsing, Alex Wiesmaier, Martín A.G. Vigil, and Johannes Buchmann</i>	
Personal PKI for the Smart Device Era	69
<i>John Lyle, Andrew Paverd, Justin King-Lacroix, Andrea Atzeni, Habib Virji, Ivan Flechais, and Shamal Faily</i>	
The Notary Based PKI	85
<i>Martín A.G. Vigil, Cristian T. Moecke, Ricardo F. Custódio, and Melanie Volkamer</i>	

Wireless Authentication and Revocation

How to Bootstrap Trust among Devices in Wireless Environments via EAP-STLS	98
<i>Massimiliano Pala</i>	
Anonymity Revocation through Standard Infrastructures	112
<i>Jesus Diaz, David Arroyo, and Francisco B. Rodriguez</i>	

Certificate and Trusted Computing

GeoPKI: Converting Spatial Trust into Certificate Trust	128
<i>Tiffany Hyun-Jin Kim, Virgil Gligor, and Adrian Perrig</i>	

Waltzing the Bear, or: A Trusted Virtual Security Module	145
<i>Ronald Toegl, Florian Reimair, and Martin Pirker</i>	

Digital Signatures

Cross-Unlinkable Hierarchical Group Signatures	161
<i>Julien Bringer, Hervé Chabanne, and Alain Patey</i>	

Non-interactive Public Accountability for Sanitizable Signatures	178
<i>Christina Brzuska, Henrich C. Pöhls, and Kai Samelin</i>	

Author Index	195
------------------------	-----