Lecture Notes in Computer Science 3545

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
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
   University of Dortmund, Germany
Madhu Sudan
   Massachusetts Institute of Technology, MA, USA
Demetri Terzopoulos
   New York University, NY, USA
Doug Tygar
   University of California, Berkeley, CA, USA
Moshe Y. Vardi
   Rice University, Houston, TX, USA
Gerhard Weikum
   Max-Planck Institute of Computer Science, Saarbruecken, Germany
Preface

This book contains the proceedings of the 2nd EuroPKI Workshop — EuroPKI 2005, held at the University of Kent in the city of Canterbury, UK, 30 June–1 July 2005. The workshop was informal and lively, and the university setting encouraged active exchanges between the speakers and the audience.

The workshop program comprised a keynote speech from Dr. Carlisle Adams, followed by 18 refereed papers, with a workshop dinner in and guided tour around the historic Dover Castle.

Dr. Adams is well known for his contributions to the CAST family of symmetric encryption algorithms, to international standards from the IETF, ISO, and OASIS, authorship of over 30 refereed journals and conference papers, and co-authorship of Understanding PKI: Concepts, Standards, and Deployment Considerations (Addison-Wesley). Dr. Adams keynote speech was entitled ‘PKI: Views from the Dispassionate “I”’, in which he presented his thoughts on why PKI has been available as an authentication technology for many years now, but has only enjoyed large-scale success in fairly limited contexts to date. He also presented his thoughts on the possible future(s) of this technology, with emphasis on the major factors hindering adoption and some potential directions for future research in these areas.

In response to the Call for Papers, 43 workshop papers were submitted in total. All papers were blind reviewed by at least two members of the Program Committee, the majority having 3 reviewers, with a few borderline papers having 4 or more reviewers; 18 papers were accepted for presentation in 8 sessions. There were sessions on: authorization, risks/attacks to PKI systems, interoperability between systems, evaluating a CA, ID ring-based signatures, new protocols, practical implementations, and long-term archiving.

I would like to thank the authors for their submitted papers, the Program Committee and external reviewers for their conscientious efforts during the review process, the Organizing Committee for their tireless efforts to ensure the smooth running of the conference, and finally all the workshop participants, without whom the workshop would not have been the success that it was.

David Chadwick
Organization

Program Chair

David Chadwick (University of Kent, UK)

Program Committee

G. Bella (University of Catania, Italy)
A. Buldas (Tallinn Technical University, Estonia)
M. Burmester (Florida State University, USA)
G. S. Cooper (University of Salford, UK)
S. De Capitani di Vimercati (University of Milan, Italy)
S. Farrell (Trinity College Dublin, Ireland)
S. Foley (University College Cork, Ireland)
S. Furnell (University of Plymouth, UK)
D. Gollmann (TU Hamburg-Harburg, Germany)
D. Gritzalis (Athens University of Economics & Business, Greece)
S. Gritzalis (University of the Aegean, Greece)
H. Imai (University of Tokyo, Japan)
S. Katsikas (University of the Aegean, Greece)
S. Kent (BBN Technologies, USA)
K. Kim (ICU, Korea)
C. Lambrinoudakis (University of the Aegean, Greece)
A. Lioy (Politecnico di Torino, Italy)
P. Lipp (IAIK, Tech. University of Graz, Austria)
J. Lopez (University of Malaga, Spain)
C. Meadows (NRL, USA)
C. Mitchell (Royal Holloway, Univ of London, UK)
R. Molva (Eurécom, France)
E. Okamoto (University of Tsukuba, Japan)
R. Oppliger (eSecurity, Switzerland)
O. Otenko (University of Kent, UK)
A. Patel (University College Dublin, Ireland)
G. Pernul (University of Regensburg, Germany)
B. Preneel (Katholieke University Leuven, Belgium)
K. Sakurai (Kyushu University Japan)
W. Schneider (Fraunhofer SIT, Germany)
S. Smith (Dartmouth College, USA)
J. P. Stern (Cryptolog, France)
M. Yung (Columbia University, USA)
J. Zhou (Institute for Infocomm Research, Singapore)
VIII Organization

Organising Chair

David Chadwick (University of Kent, UK)

Organising Committee

Uche Mbanaso (University of Salford, UK)
Tuan Anh Nguyen (University of Kent, UK)
Jenny Oatley (University of Kent, UK)
Wensheng Xu (University of Kent, UK)
Gansen Zhao (University of Kent, UK)

External Reviewers

George Angelis (University of the Aegean, Greece)
George Kambourakis (University of the Aegean, Greece)
Dimitris Lekkas (University of the Aegean, Greece)
John Iliadis (University of the Aegean, Greece)
Thomas Pornin (Cryptolog International, France)
Lazaros Gymnopoulous (University of the Aegean, Greece)
Dimitris Geneiatakis (University of the Aegean, Greece)
Mario Lamberger (IAIK/Stiftung SIC, Austria)
Bin Zhang (Chinese Academy of Sciences, China)
Torsten Priebe (University of Regensburg, Germany)
Bjoern Muschall (University of Regensburg, Germany)
Christian Schläger (University of Regensburg, Germany)
Margus Freudenthal (Cybernetica, Estonia)
Jose A. Montenegro (University of Malaga, Spain)
Thomas Quillianan (University College Cork, Ireland)
Gregory Neven (Katholieke Universiteit Leuven, Belgium)
Yoshifumi Ueshige (Institute of Systems & Information Technologies, Japan)
# Table of Contents

## Authorisation

A Multipurpose Delegation Proxy for WWW Credentials  
*Tobias Straub, Thilo-Alexander Ginkel, Johannes Buchmann*  
1

Secure Role Activation and Authorization in the Enterprise Environment  
*Richard W.C. Lui, Lucas C.K. Hui, S.M. Yiu*  
22

Towards a Unified Authentication and Authorization Infrastructure for Grid Services: Implementing an Enhanced OCSP Service Provider into GT4  
*Jesus Luna, Manel Medina, Oscar Manso*  
36

## Interoperability

A Heterogeneous Network Access Service Based on PERMIS and SAML  
*Gabriel López, Óscar Cánovas, Antonio F. Gómez-Skarmeta, Sassa Otenko, David W. Chadwick*  
55

Interoperation Between a Conventional PKI and an ID-Based Infrastructure  
*Geraint Price, Chris J. Mitchell*  
73

XKMS Working Group Interoperability Status Report  
*Guillermo Álvaro, Stephen Farrell, Tommy Lindberg, Roland Lockhart, Yunhao Zhang*  
86

## Evaluating a CA

An Innovative Policy-Based Cross Certification Methodology for Public Key Infrastructures  
*Valentina Casola, Antonino Mazzeo, Nicola Mazzocca, Massimiliano Rak*  
100

Modeling Public Key Infrastructures in the Real World  
*John Marchesini, Sean Smith*  
118
Classifying Public Key Certificates
   *Javier Lopez, Rolf Oppliger, Günther Pernul* ........................... 135

**ID Based Ring Signatures**

Identity Based Ring Signature: Why, How and What Next
   *Sherman S.M. Chow, Richard W.C. Lui, Lucas C.K. Hui,
   S.M. Yiu* .......................... 144

**Practical Implementations**

Development of a Flexible PERMIS Authorisation Module for Shibboleth and Apache Server
   *Wensheng Xu, David W. Chadwick, Sassa Otenko* .................... 162

CA-in-a-Box
   *Mark Franklin, Kevin Mitcham, Sean Smith, Joshua Stabiner,
   Omen Wild* ........................... 180

**New Protocols**

A Lower-Bound of Complexity for RSA-Based Password-Authenticated Key Exchange
   *SeongHan Shin, Kazukuni Kobara, Hideki Imai* .................... 191

Recoverable and Untraceable E-cash
   *Joseph K. Liu, Patrick P. Tsang, Duncan S. Wong* ............. 206

**Risks and Attacks**

A Method for Detecting the Exposure of OCSP Responder’s Session Private Key in D-OCSP-KIS
   *Younggyo Lee, Injung Kim, Seungjoo Kim, Dongho Won* ............ 215

Installing Fake Root Keys in a PC
   *Adil Alsaid, Chris J. Mitchell* ........................... 227

**Long Term Archiving**

Provision of Long-Term Archiving Service For Digitally Signed Documents Using an Archive Interaction Protocol
   *Aleksej Jerman Blazic, Peter Sylvester* ........................... 240