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 Chadwick Gansen Zhao (Eds.)

Public Key Infrastructure

Second European PKI Workshop:
Research and Applications, EuroPKI 2005
Canterbury, UK, June 30 - July 1, 2005
Revised Selected Papers

Springer

Volume Editors

David Chadwick
Gansen Zhao
University of Kent, The Computing Laboratory
Canterbury CT2 7NF, UK
E-mail: {d.w.chadvick,gz7}@kent.ac.uk

Library of Congress Control Number: 2005935450

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-10 3-540-28062-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28062-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11533733 06/3142 5 4 3 2 1 0

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 Corke, 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 (Eurècom, 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)

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 Gymnopoulos (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 Quillinan (University College Cork, Ireland)
Gregory Neven (Katholieke Universiteit Leuven, Belgium)
Yoshifumi Ueshige (Institute of Systems & Information Technologies, Japan)

Table of Contents

Authorisation

Interoperability

Evaluating a CA

ID Based Ring Signatures

Practical Implementations

New Protocols

Risks and Attacks

Long Term Archiving