Lecture Notes in Computer Science 3225

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

Editorial Board

Kan Zhang Yuliang Zheng (Eds.)

Information Security

7th International Conference, ISC 2004
Palo Alto, CA, USA, September 27-29, 2004
Proceedings

Springer

Volume Editors

Kan Zhang
Hewlett-Packard Laboratories
3353 Alma Street, #233, Palo Alto, CA 94306, USA
E-mail: zhangkan@sbcglobal.net

Yuliang Zheng
University of Noth Carolina at Charlotte
Department of Software and Information Systems
9201 University City Blvd, Charlotte, NC 28223, USA
E-mail: yzheng@uncc.edu

Library of Congress Control Number: 2004112165

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-23208-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11325864 06/3142 5 4 3 2 1 0

Preface

The 2004 Information Security Conference was the seventh in a series that started with the Information Security Workshop in 1997. A distinct feature of this series is the wide coverage of topics with the aim of encouraging interaction between researchers in different aspects of information security. This trend continued in the program of this year's conference. The program committee received 106 submissions, from which 36 were selected for presentation. Each submission was reviewed by at least three experts in the relevant research area. We would like to thank all the authors for taking their time to prepare the submissions, and we hope that those whose papers were declined will be able to find an alternative forum for their work.

We were fortunate to have an energetic team of experts who took on the task of the program committee. Their names may be found overleaf, and we thank them warmly for their time and efforts. This team was helped by an even larger number of external reviewers who reviewed papers in their particular areas of expertise. A list of these names is also provided, which we hope is complete.

We would also like to thank the advisory committee for their advice and support. The excellent local arrangements were handled by Dirk Balfanz and Jessica Staddon. We made use of the electronic submission and reviewing software supplied by COSIC at the Katholieke Universiteit Leuven. Both the software and the ISC 2004 website were run on a server at UNC Charlotte, and were perfectly maintained by Seung-Hyun Im. We also appreciate assistance from Lawrence Teo in editing the proceedings.

September 2004

Kan Zhang
Yuliang Zheng

Information Security Conference 2004

September 27–29, 2004, Palo Alto, CA, USA

General Chair

Yuliang Zheng, University of North Carolina at Charlotte, USA

Advisory Committee

Tom Berson, Anagram Lab, USA
Li Gong, Sun Microsystems, China
Wenbo Mao, Hewlett-Packard Laboratories, UK
Eiji Okamoto, University of Tsukuba, Japan

Program Co-chairs

Kan Zhang, Hewlett-Packard Laboratories, USA
Yuliang Zheng, University of North Carolina at Charlotte, USA

Program Committee

Martin Abadi ..... UC Santa Cruz, USA
Carlisle Adams ..... University of Ottawa, Canada
Gail-Joon Ahn ..... UNC Charlotte, USA
N. Asokan ..... Nokia, Finland
Tuomas Aura ..... Microsoft Research, UK
Jean Bacon ..... Cambridge University, UK
Dirk Balfanz ..... PARC, USA
Feng Bao ..... i2r, Singapore
Elisa Bertino ..... University of Milan, Italy
Colin Boyd ..... QUT, Australia
Yvo Desmedt ..... University College London, UK
Warwick Ford ..... Verisign, USA
Craig Gentry ..... NTT DoCoMo Labs, USA
Stuart Haber ..... HP Labs, USA
Markus Jakobsson ..... RSA Labs, USA
Marc Joye ..... Gemplus, France
Michiharu Kudoh ..... IBM Tokyo, Japan
Javier Lopez ..... University of Malaga, Spain
Tsutomu Matsumoto ..... Yokohama National University, Japan
Kanta Matsuura ..... University of Tokyo, Japan
Catherine Meadows ..... Naval Research Lab, USA
Jonathan Millen ..... SRI International, USA
John Mitchell ..... Stanford University, USA
Peng Ning ..... North Carolina State University, USA
Joe Pato ..... HP Labs, USA
Josef Pieprzyk ..... Macquarie University, Australia
Jean-Jacques Quisquater ..... UCL, Belgium

External Reviewers

Table of Contents

Intrusion Detection

Access Control

Human Authentication

Certificate Management

Mobile and Ad Hoc Security

Web Security

Digital Rights Management

Software Security