Lecture Notes in Computer Science 2727

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Rei Safavi-Naini Jennifer Seberry (Eds.)

Information Security and Privacy

8th Australasian Conference, ACISP 2003
Wollongong, Australia, July 9-11, 2003
Proceedings

Springer

Volume Editors

Rei Safavi-Naini
Jennifer Seberry
University of Wollongong
School of Information Technology and Computer Science
Wollongong, NSW 2522, Australia
E-mail: {rei,jennifer_seberry}@uow.edu.au

Cataloging-in-Publication Data applied for

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

ISSN 0302-9743
ISBN 3-540-40515-1 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH
Printed on acid-free paper SPIN: 10929049 06/3142 5 4 3 2 1 0

Preface

The 8th Australasian Conference on Information Security and Privacy (ACISP 2003) was held in Wollongong, 9–11 July, 2003. The conference was sponsored by the Australasian Computer Society, the School of Information Technology and Computer Science of the University of Wollongong, and the Smart Internet Technology Collaborative Research Centre. The conference was organized cooperatively with the IEEE-CS Task Force on Information Assurance.

The conference brought together researchers and practitioners, from academia, industry and government, with interests in information security and privacy. The conference program included 42 papers covering a wide range of topics including cryptography and cryptanalysis, network security and system security. The papers were selected from 158 submissions after an extensive and careful refereeing process in which each paper was reviewed by at least 3 members of the program committee. Of the accepted papers there were 11 from Korea, 9 from Japan, 6 from Australia, 3 from Taiwan, 2 each from Singapore and the USA, and 1 each from Canada, China, Denmark, France, Germany, India, Italy, Saudi Arabia, and Spain.

There were four invited speakers for the conference: Prof. Andrew Odlyzko (Digital Media Center, University of Minnesota, USA), Prof. Chris Mitchell (Information Security Group, Royal Holloway, University of London, UK), Dr. Li Gong (Sun Microsystems), and Prof. Gerard Milburn (University of Queensland, Australia).

We appreciate the diligence and hard work of the ACISP 2003 Program Committee. The committee benefited from the reviews and comments of many other experts: Aggelos Kiayias, Alex Dent, Alice Silverberg, Anand Desai, Andrew Clark, Atsuko Miyaji, Atsushi Fujioka, Beatrice Peirani, Bill Millan, Carine Boursier, Chi-Jen Lu, Chieng-Ning Chen, Chong Hee Kim, Christophe Tymen, Claude Carlet, Dae Hyun Yum, Darrel Hankerson, Dong Jin Park, Dong To, Drew Dean, Eiichiro Fujisaki, Eric Brier, Eric Chen, Fabienne Cathala, Gareth Brisbane, Gary Carter, Geraint Price, Gildas Avoine, Glenn Durfee, Gonzalvo Benoit, Greg Maitland, Hao-Chi Wong, Helena Handschu, Hsi-Chung Lin, Huaxiong Wang, Hung-Min Sun, In Kook Park, Jason Crampton, Jason Reid, Jean Monnerat, Jean-Sebastien Coron, Ji Hyun Jeong, John Proos, Jong Hoon Shin, Juan Manuel Gonzalez Nieto, Julien Brouchier, Kapali Viswanathan, Kazumaro Aoki, Khanh Nguyen, Koji Chida, Koji Chida, Koutarou Suzuki, Laurent Gauteron, Lionel Victor, Lu Yi, Ludovic Rousseau, Marc Joye, Mariusz Jakabowski, Mark Bauer, Mark Looi, Matt Henricksen, Min-Shiang Hwang, Nicholas Sheppard, Nicolas Courtois, Oleg Sheyner, Pascal Junod, Pascal Paillier, Philippe Oechslin, Pierre Girard, Ron Steinfeld, Sang Gyoo Sim, Sang Yun Han, Satomi Okazaki, Scarlet Schwiderski-Grosche, Shin'ichiro Matsuo, Simon Blackburn, Siu-Leung Chung, Svein Knapskog, Swee-Huay Heng, Takayuki Yamada, Teresa Lunt, Tetsu Iwata, Thomas Martin, Tung-Shou Chen, Wataru Kishimoto,

Willy Susilo, Xianmo Zhang, Xuli Wang, Yasuhiro Ohtaki, Yeon Hyeong Yang, Yi Lu, Yong Ho Hwang, and Zhi Guo.

The organizing committee was co-chaired by Dr. Willy Susilo and Prof. Jennifer Seberry. Special thanks to Takeyuki Uehara, Rongbo Du and Stephen Haynes for their technical support, to Takeyuki Uehara and Yejing Wang for their help with the local organization, and the following volunteers whose help allowed us to run the conference smoothly: Hartono Kurnio, Luke McAven, Nicholas Sheppard, Tianbing Xia, Nathan Curtis, David Haryanto, Yibing Kong, Gelareh Taban, and Rungrat Wiangsripanawan.

On behalf of all those involved in organizing the conference, we would like to thank the authors of all submitted papers, those who presented their work and those who participated in the conference: their work and contributions made the conference a great success.

July 2003 Rei Safavi-Naini

Australasian Conference on Information Security and Privacy
ACISP 2003

Sponsored by
School of Information Technology and Computer Science of the
University of Wollongong
Australian Computer Society
Smart Internet Technology Cooperative Research Centre

In cooperation with
IEEE-CS Task Force on Information Assurance

General Chairs

Jennifer Seberry	*University of Wollongong, Australia*
Willy Susilo	*University of Wollongong, Australia*

Program Chair

Rei Safavi-Naini	*University of Wollongong, Australia*

Program Committee

Masayuki Abe	*NTT, Japan*
Lynn Batten	*Deakin University, Australia*
Colin Boyd	*Queensland University of Technology, Australia*
Ed Dawson	*Queensland University of Technology, Australia*
Dieter Gollmann	*Microsoft, UK*
Jim Hughes	*StorageTek, US*
Kaoru Kurosawa	*Ibaraki University, Japan*
Kwok-Yan Lam	*Tsinghua University, China*
Chi-Sung Laih	*National Cheng Kung University, Taiwan*
Pil Joong Lee	*Pohang University of Science and Technology, Korea*
Keith Martin	*Royal Holloway, University of London, UK*
Mitsuru Matsui	*Mitsubishi Electric, Japan*
Alfred Menezes	*University of Waterloo, Canada*
Yi Mu	*University of Wollongong, Australia*
David Naccache	*Gemplus, France*

Dingyi Pei	*Chinese Academy of Sciences, China*
Josef Pieprzyk	*Macquarie University, Australia*
Pandu Rangan	*Indian Institute of Technology, Madras, India*
Greg Rose	*Qualcomm, Australia*
Jessica Staddon	*Palo Alto Research Center, US*
Vijay Varharadjan	*Macquarie University, Australia*
Serge Vaudeney	*EPFL* (*Swiss Fed. Inst. of Tech. Lausanne*), *Switzerland*
Eric Verheul	*PricewaterhouseCoopers, The Netherlands*
Chee Sun Won	*Dongguk University, Korea*
Sung-Ming Yen	*National Central University, Taiwan*
Moti Yung	*Columbia University, US*

Table of Contents

Mobile and Network Security

Invited Talk (II)

Cryptanalysis (II)

Signature

Cryptosystems (I)

Invited Talk (III)

Cryptosystems (II)

Key Management

Theory and Hash Functions