Lecture Notes in Computer Science 4586

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

Josef Pieprzyk Hossein Ghodosi
Ed Dawson (Eds.)

Information Security and Privacy

12th Australasian Conference, ACISP 2007
Townsville, Australia, July 2-4, 2007
Proceedings

Springer

Volume Editors

Josef Pieprzyk
Macquarie University, Department of Computing
Center for Advanced Computing - Algorithms and Cryptography
Sydney, NSW 2109, Australia
E-mail: josef@ics.mq.edu.au

Hossein Ghodosi
James Cook University
School of Mathematics, Physics, and Information Technology
Townsville, QLD 4811, Australia
E-mail: hossein@cs.jcu.edu.au

Ed Dawson
Queensland University of Technology, Information Security Institute
Brisbane, QLD 4001, Australia
E-mail: e.dawson@qut.edu.au

Library of Congress Control Number: 2007929635

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-73457-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-73457-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12086818 06/3180 5 4 3 2 1 0

Preface

The 12th Australasian Conference on Information Security and Privacy—ACISP2007—was held in Townsville, Queensland, July 2–4, 2007. This was the first conference to be organized outside the traditional three venues: Brisbane and Gold Coast, Melbourne, and Sydney and Wollongong. The conference was sponsored by James Cook University, Center for Advanced Computing – Algorithm and Cryptography at Macquarie University, Information Security Institute at Queensland University of Technology, and the Research Network for Secure Australia. We would like to thank Matthieu Finiasz and Thomas Baignères from EPFL, LASEC, Switzerland for letting us use their iChair software that facilitated the submission and revision processes.

Out of 132 submissions, the Program Committee (PC) selected 33 papers after a rigorous review process. Each paper got assigned to at least three referees. Papers submitted by members of the PC got assigned to five referees. In the first stage of the review process, the submitted papers were read and evaluated by the PC members and then in the second stage, the papers were scrutinized during a three-week-long discussion. We would like to thank the authors of all papers (both accepted and rejected) for submitting their papers to the conference. A special thanks go to the members of the PC and the external referees who gave their time, expertise and enthusiasm in order to select the best collection of papers.

As in previous years, we held a competition for the "best student paper." To be eligible, a paper had to be co-authored by a postgraduate student whose contribution was more than 50%. Eight papers entered the competition. The winner was Norbert Pramstaller from Graz University of Technology, Austria, for the paper "Second Preimages for Iterated Hash Functions and Their Implications on MACs."

This year we had only one invited talk, which was given by Andreas Enge. The title of the talk was "Contributions Cryptographic Curves."

We would like to express our thanks to Springer and in particular, to Alfred Hofmann and Ronan Nugent for their continuing support of the ACISP conference and for help in the conference proceeding production. Further, we thank Michelle Kang, who helped us with the setting up and maintenance of the ACISP Web site, Vijayakrishnan Pasupathinathan, who took care of the iChair server and ACISP mailbox, Adam Shah for installation of the iChair server and Elizabeth Hansford for assisting with conference organization.

July 2007

Josef Pieprzyk
Hossein Ghodosi
Ed Dawson

Organization

ACISP 2007

July 2–4, 2007, Townsville, Queensland, Australia

General Co-chairs

Hossein Ghodosi	James Cook University, Australia
Ed Dawson	QUT, Australia

Program Chair

Josef Pieprzyk	Macquarie University, Australia

Program Committee

Paul Ashley	IBM, Australia
Tuomas Aura	Microsoft, USA
Lynn Batten	Deakin University, Australia
Colin Boyd	QUT, Australia
Andrew Clark	QUT, Australia
Scott Contini	Macquarie University, Australia
Nicolas Courtois	University College London, UK and Gemalto, France
Yvo Desmedt	University College London, UK
Christophe Doche	Macquarie University, Australia
Ed Dawson	QUT, Australia
Hossein Ghodosi	James Cook University, Australia
Jovan Golić	Telecom, Italy
Dieter Gollmann	TUHH, Germany
Peter Gutmann	University of Auckland, New Zealand
Kwangjo Kim	ICU, Korea
Sevin Knapskog	NTNU, Norway
Kaoru Kurosawa	Ibaraki University, Japan
Tanja Lange	TU/e, Netherlands
Javier Lopez	University of Malaga, Spain
Keith Martin	Royal Holloway, UK
Mitsuru Matsui	Mitsubishi Electric, Japan
Paul Montague	Motorola, Australia
Yi Mu	University of Wollongong, Australia
Andrew Odlyzko	University of Minnesota, USA
Eiji Okamoto	University of Tsukuba, Japan
Rafail Ostrovsky	UCLA, USA

David Poincheval	ENS, France
Bart Preneel	K.U.Leuven, Belgium
Bimal Roy	ISICAL, India
Rei Safavi-Naini	University of Wollongong, Australia
	University of Calgary, Canada
Jennifer Seberry	University of Wollongong, Australia
Igor Shparlinski	Macquarie University, Australia
Ron Steinfeld	Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Henk van Tilborg	TU/e, Netherlands
Serge Vaudenay	EPFL, Switzerland
Huaxiong Wang	Macquarie University, Australia
	Nanyang Technological University, Singapore
Henry Wolfe	University of Otago, New Zealand

External Reviewers

Ajith Abraham	Avishek Adhikari	Isaac Agudo
Man Ho Au	Joonsang Baek	Vittorio Bagini
Yun Bai	Thomas Baignères	Rana Barua
Daniel J. Bernstein	Peter Birkner	Xavier Boyen
Yang Cui	Jan Camenisch	Christophe De Cannière
Alvaro Cardenas	Dario Catalano	Agnes Chan
Chris Charnes	Benoit Chevallier-Mames	Sherman S. M. Chow
Yvonne Cliff	Tanmoy Das	Pascal Delaunay
Dang Nguyen Duc	Ernest Foo	Pierre-Alain Fouque
Jun Furukawa	Krzysztof M. Gaj	David Galindo
Juan Garay	Danilo Gligoroski	M. Choudary Gorantla
Jens Groth	Kishan Chand Gupta	Goichiro Hanaoka
Kjetil Haslum	Swee-Huay Heng	Jonathan Herzog
Shoichi Hirose	Michael Hitchens	Jeffrey Horton
Xinyi Huang	Laurent Imbert	Sebastiaan Indesteege
Mahabir Prasad Jhanwar	Emilia Käsper	Lars R. Knudsen
Markulf Kohlweiss	Divyan M. Konidala	Takeshi Koshiba
Kerstin Lemke-Rust	Vo Duc Liem	Chu-Wee Lim
Liang Liu	Liang Lu	Anna Lysyanskaya
Mark Manulis	Abe Masayuki	Krystian Matusiewicz
Luke McAven	Miodrag Mihaljevic	Ilya Mironov
Guglielmo Morgari	Sean Murphy	Pablo Najera
Gregory Neven	Antonio Nicolosi	Svetla Nikova
Wakaha Ogata	Jose A. Onieva	Dunkelman Orr
Pascal Paillier	Sylvain Pasini	Kenny Paterson
Maura Paterson	Goutam Paul	Souradyuti Paul
Kun Peng	Slobodan Petrovic	Raphael C.-W. Phan
Le Trieu Phong	Geraint Price	Havard Raddum

Mohammad Reza Reyhanitabar
Chun Ruan
Siamak Shahandashti
Makoto Sugita
Qiang Tang
Toshio Tokita
Frederik Vercauteren
Guilin Wang
Yan Wang
Benne de Weger
Qianhong Wu
Qingsong Ye
Sèbastien Zimmer

Rodrigo Roman
Yasuyuki Sakai
Nicholas Sheppard
Daisuke Suzuki
Christophe Tartary
Jacques Traore
Charlotte Vikkelsoe
Peishun Wang
Yongge Wang
Christopher Wolf
Guangwu Xu
Hongbo Yu

Greg Rose
Somitra Sanadhya
Jason Smith
Katsuyuki Takashima
Clark Thomborson
Pim Tuyls
Martin Vuagnoux
Shuhong Wang
Brent Waters
Hongjun Wu
Bo-Yin Yang
Steve Zdancewic

Table of Contents

Cryptanalysis

Public Key Cryptography

Authentication

E-Commerce

Security