Lecture Notes in Computer Science 5107

Yi Mu   Willy Susilo   Jennifer Seberry (Eds.)

Information Security and Privacy

13th Australasian Conference, ACISP 2008
Wollongong, Australia, July 7-9, 2008
Proceedings

Springer

Volume Editors

Yi Mu
Willy Susilo
Jennifer Seberry
University of Wollongong
School of Computer Science and Software Engineering
Northfields Avenue, Wollongong, NSW 2522, Australia
E-mail: {ymu, wsusilo, jennie}@uow.edu.au

Library of Congress Control Number: Applied for

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 3-540-69971-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-69971-2 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12322725 06/3180 5 4 3 2 1 0

Preface

The 13th Australasian Conference on Information Security and Privacy (ACISP 2008) was held at Wollongong, Australia, during July 7–9, 2008. The conference was sponsored by the Centre for Computer and Information Security of the University of Wollongong and the Research Network for a Secure Australia. The submission and review process was run using the iChair software, written by Thomas Baigneres and Matthieu Finiasz from EPFL, LASEC, Switzerland. We would like to thank them for letting us use their iChair software.

The conference received 111 submissions, out of which the Program Committee selected 33 papers for presentation at the conference after a rigorous review process. These papers are included in the proceedings. The accepted papers cover a range of topics in information security, including authentication, key management, public key cryptography, privacy, anonymity, secure communication, ciphers, network security, elliptic curves, hash functions, and database security. The conference proceedings contain revised versions of the selected papers. Since some of them were not checked again for correctness before publication, the authors bear full responsibility for the contents of their papers. We would like to thank the authors of all papers for submitting their papers to the conference.

In addition to the contributed papers, the program comprised three invited talks. The invited speakers were Xavier Boyen (Voltage, USA), Josef Pieprzyk (Macquarie University, Australia) and Nigel Phair (Australian High Tech Crime Centre). We would like to express our thanks to them.

As in previous years, we selected a “best student paper.” To be eligible for selection, a paper has to be co-authored by a postgraduate student, whose contribution was more than 50%. The winner was Risto Hakala from Helsinki University of Technology, Finland, for the paper “Linear Distinguishing Attack on Shannon.”

We would like to thank all the people who helped with the conference program and organization. In particular, we heartily thank the Program Committee and the sub-reviewers listed on the following pages for the effort and time they contributed to the review process. We would like to express our thanks to Springer for continuing to support the ACISP conference and for help in the conference proceedings production.

Finally, we would like to thank the Organizing Committee for their excellent contribution to the conference.

July 2008

Yi Mu
Willy Susilo
Jennifer Seberry

The 13th Australasian Conference on Information Security and Privacy (ACISP 2008)

Sponsored by

Centre for Computer and Information Security Research,
University of Wollongong, Australia

Research Network for a Secure Australia

General Chair

Jennifer Seberry	University of Wollongong, Australia

Program Chairs

Yi Mu	University of Wollongong, Australia
Willy Susilo	University of Wollongong, Australia

Program Committee

Michel Abdalla	ENS, Paris, France
Masayuki Abe	NTT, Japan
Colin Boyd	QUT, Australia
Feng Bao	Institute for Infocomm Research, Singapore
Lynn Batten	Deakin University, Australia
Ed Dawson	QUT, Australia
Dieter Gollmann	TU Hamburg, Germany
Aggelos Kiayias	University of Connecticut, USA
Kwangjo Kim	ICU, Korea
Tanja Lange	Technische Universiteit Eindhoven, Netherlands
Pil Joong Lee	Pohang University of Science and Technology, Korea
Benoit Libert	UCL, Belgium
Javier Lopez	University of Malaga, Spain
Chris Mitchell	RHUL, UK
Yi Mu	University of Wollongong, Australia
Kaisa Nyberg	Helsinki University of Technology, Finland
Eiji Okamoto	Tsukuba University, Japan
Josef Pieprzyk	Macquarie University, Australia
Sihan Qing	Chinese Academy of Scineces, China
Jean-Jacques Quisquater	UCL, Belgium
Rei Safavi-Naini	University of Calgary, Canada

Jennifer Seberry	University of Wollongong, Australia
Ron Steinfeld	Macquarie University, Australia
Douglas Stinson	University of Waterloo, Canada
Willy Susilo	University of Wollongong, Australia
C. Pandu Rangan	Indian Institute of Technology, India
Tsuyoshi Takagi	Future University, Japan
Vijay Varadharajan	Macquarie University, Australia
Sabrina De Capitani di Vimercati	University of Milan, Italy
Huaxiong Wang	Nanyang Technological University, Singapore
Duncan S. Wong	City University of Hong Kong, China
Fangguo Zhang	Sun Yat-Sen University, China
Ning Zhang	University of Manchester, UK
Jianying Zhou	Institute for Infocomm Research, Singapore

Organizing Committee

Man Ho Au	University of Wollongong, Australia
Xinyi Huang	University of Wollongong, Australia
Shams Ud Din Qazi	University of Wollongong, Australia
Mohammad Reza Reyhanitabar	University of Wollongong, Australia
Siamak Fayyaz Shahandashti	University of Wollongong, Australia
Pairat Thorncharoensri	University of Wollongong, Australia
Wei Wu	University of Wollongong, Australia
Tsz Hon Yuen	University of Wollongong, Australia

External Referees

Isaac Agudo
Hadi Ahmadi
K. Ambika
Venkat Balakrishnan
Daniel J. Bernstein
Jean-Luc Beuchat
Peter Birkner
Billy Bob Brumley
S. Chandrasekar
Joo Yeon Cho
Sherman Chow
Baudoin Collard
Alex Dent
Dang Nguyen Duc
Sung Wook Eom
Reza Rezaeian Farashahi
Gerardo Fernandez
Carmen Fernandez-Gago
Georg Fuchsbauer
Juan Garay
Praveen Gauravaram
Juan Gonzalez
Satoshi Hada
Risto Hakala
Kevin Henry
Matt Henricksen
Jason Hinek
Michael Hitchens
Qiong Huang
Shaoquan Jiang
Jang Seong Kim
Sun Young Kim
Young Mok Kim
Varad Kirthane
Hoi Le
Fagen Li
Jin Li
Vo Duc Liem
Peter van Liesdonk
Joseph K. Liu
Jiqiang Lu
Mark Manulis
Krystian Matusiewicz
Antonina Mitrofanova
Cameron McDonald

Pablo Najera
Miyako Ohkubo
Vijayakrishnan P.
Arpita Patra
Angela Piper
M.R. Reyhanitabar
Rodrigo Roman
Chun Ruan
Palash Sarkar
Sharmila Devi Selvi
Jae Woo Seo
Siamak Shahandashti
Hongsong Shi
Jong Hoon Shin
Masaaki Shirase
Igor Shparlinski
Leonie Simpson
Michal Sramka
Jerry Sui
Christophe Tartary
Ronghua Tian
Tomas Toft
Mohammed A.A. Tuhin
Udaya Kiran Tupakula
Damien Vergnaud
José Villegas
Jose L. Vivas
Yongge Wang
Baodian Wei
Kenneth Wong
Jiang Wu
Guomin Yang
Yanjiang Yang
Yeon-Hyeong Yang
Chan Yeob Yeun
Hongbo Yu
Yu Yu
Janson Zhang
Chang-An Zhao
Weiliang Zhao
Hong-Sheng Zhou
Huafei Zhu
Sebastien Zimmer

Table of Contents