Lecture Notes in Computer Science 4058

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

Lynn Margaret Batten
Reihaneh Safavi-Naini (Eds.)

Information Security and Privacy

11th Australasian Conference, ACISP 2006
Melbourne, Australia, July 3-5, 2006
Proceedings

Springer

Volume Editors

Lynn Margaret Batten
Deakin University
221 Burwood Highway, Burwood 3125, Victoria, Australia
E-mail: lmbatten@deakin.edu.au

Reihaneh Safavi-Naini
University of Wollongong
Centre for Information Security
Wollongong, NSW 2519, Australia
E-mail: rei@uow.edu.au

Library of Congress Control Number: 2006927435

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 3-540-35458-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-35458-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11780656 06/3142 5 4 3 2 1 0

Preface

The 11th Australasian Conference on Information Security and Privacy (ACISP 2006) was held in Melbourne, 3–5 July, 2006. The conference was sponsored by Deakin University, the Research Network for a Secure Australia, and was organized in cooperation with the University of Wollongong. The conference brought together researchers, practitioners and a wide range of other users from academia, industries and government organizations.

The program included 35 papers covering important aspects of information security technologies. The papers were selected from 133 submissions through a two-stage anonymous review process. Each paper received at least three reviews by members of the Program Committee, and was then scrutinized by the whole committee during a two-week discussion. There were 19 papers eligible for the "best student paper" award. The award was given to Yang Cui from the University of Tokyo for the paper "Tag-KEM from Set Partial Domain One-Way Permutations."

In addition to the regular papers the program also included three invited talks. Bart Preneel gave an invited talk entitled "Electronic Identity Cards: Threats and Opportunities." Mike Burmester's talk was "Towards Provable Security for Ubiquitous Applications." The details of the third talk had not been finalized at the time of publication of these proceedings.

We wish to thank all the authors of submitted papers for providing the content for the conference; their high-quality submissions made the task of selecting a program very difficult. We are indebted to the diligence and enthusiasm of the Program Committee members in ensuring selection of the most deserving papers and to the external reviewers who helped in the refereeing process. We wish to thank our sponsors, Research Network for a Secure Australia, for their support of the main speakers and students as well as Springer for their continued support of ACISP. We further wish to thank Judy Chow, the conference secretary, for her many organizational skills and patience with the registration process, and our Technical Chair, Jeffrey Horton, for his continuous effort and meticulous attention to every detail, which made the task of the Program Co-chairs so much easier.

Without the help of all the above this conference would not have been a possibility.

July 2006

Lynn Batten
Reihaneh Safavi-Naini

ACISP 2006

July 3–5, 2006, Melbourne, Australia

General Chair
Lynn Batten, Deakin University, Australia

Program Co-chairs
Lynn Batten, Deakin University, Australia
Reihaneh Safavi-Naini, University of Wollongong, Australia

Technical Chair
Jeffrey Horton, University of Wollongong, Australia

Program Committee

Tuomas Aura	Microsoft Research, UK
Feng Bao	Institute for Infocomm Research, Singapore
Colin Boyd	QUT, Australia
Liqun Chen	Hewlett-Packard Laboratories, UK
Kefei Chen	Shanghai Jiaotong University, China
Nicolas T. Courtois	Axalto Smart Cards, France
Robert Deng	Singapore Management University, Singapore
Marc Dacier	Eurecom Institute, France
Ed Dawson	QUT, Australia
Josep Domingo	University of Tarragona, Catalonia
Dieter Gollmann	Hamburg University of Technology, Germany
Juan Gonzalez Nieto	QUT, Australia
Goichiro Hanaoka	Nat. Inst. of Adv. Industrial Sci. and Tech., Japan
Markus Jakobsson	Indiana University, USA
Marc Joye	Gemplus & CIM-PACA, France
Tanja Lange	Technical University of Denmark, Denmark
Byoungcheon Lee	Joongbu University, Korea
Javier Lopez	University of Malaga, Spain
Subhamoy Maitra	Indian Statistical Institute, Kolkata, India
Catherine Meadows	Naval Research Lab, USA
Atsuko Miyaji	JAIST, Japan
Nasir Memon	New York Polytechnic, USA
SangJae Moon	Kyungpook National University, Korea
Keith Martin	Royal Holloway, University of London, UK
Peng Ning	North Carolina State University, USA
Kaisa Nyberg	Helsinki University of Technology and Nokia, Finland
Eiji Okamoto	Tsukuba University, Japan
Giuseppe Persiano	Università di Salerno, Italy
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	CNRS/ENS, Paris, France
Bimal Roy	Indian Statistical Institute, Kolkata, India
Palash Sarkar	Indian Statistical Institute, India

Jennifer Seberry	University of Wollongong, Australia
Juji Shikata	Yokohama National University, Japan
Nigel Smart	University of Bristol, UK
Douglas Stinson	University of Waterloo, Canada
Tim Strayer	BBN Technologies, USA
Clark Thomborson	University of Auckland, New Zealand
Serge Vaudenay	EPFL, Switzerland
Vijay Varadharajan	Macquarie University, Australia
Victor K. Wei	Chinese University of Hong Kong, Hong Kong

External Reviewers

Masayuki Abe
Joel Alwen
Nuttapong Attrapadung
Roberto M. Avanzi
Gildas Avoine
Thomas Baignères
Daniel J. Bernstein
Srimanta Bhattacharya
Olivier Billet
Mark Branagan
Emmanuel Bresson
Jaimee Brown
Billy Brumley
Debrup Chakraborty
Zhaohui Cheng
Andrew Clark
Christophe Clavier
Yvonne Cliff
Scott Contini
Yang Cui
Paolo D'Arco
Vanesa Daza
Ling Dong
Ratna Dutta
Stefan Dziembowski
Sarah Edwards
Mari Carmen Fernandez-Gago
Matthieu Finiasz
Eiichiro Fujisaki
Jun Furukawa
Clemente Galdi
Zheng Gong
Aline Gouget
Vanessa Gratzer
Jens Groth
JaeCheol Ha
Matt Henricksen
Jason Hinek
Xuan Hong
Zhenjie Huang
Sarath Indrakanti
Toshiyuki Isshiki
Tetsuya Izu
Christine Jones
Ari Juels
Lars Knudsen
Sandeep Kumar
Noboru Kunihiro
Kaoru Kurosawa
Eyal Kushilevitz
David Lapsley
Jens Ove Lauf
HoonJae Lee
Corrado Leita
Qiming Li
Ching Lin
Joseph Liu
Carl Livadas
Yu Long
Yi Lu
John Malone-Lee
Antoni Martínez-Ballesté
Sebastia Martin
Krystian Matusiewicz
Bill Millan
Hideyuki Miyake
Kunihiko Miyazaki
Jean Monnerat
Mridul Nandy
Stan Nurislov
Wakaha Ogata
Juan J. Ortega
Akira Otsuka
Vikram PAdman
Dan Page
Sylvain Pasini
Ahmed Patel
Kenny Paterson
Kun Peng
Pai Peng
Krzysztof Pietrzak
Jordi Castellà Roca
Rodrigo Roman
Kurt Rosenfeld
Chun Ruan
Naouel Ben Salem
Sumanta Sarkar
Francesc Sebé
Taha Sencar
Abdulattif Shikfa
SeongHan Shin
Leonie Simpson
Agustí Solanas
Masakazu Soshi
Ron Steinfeld
Gene Tsudik
Udaya Kiran Tupakula
Ivan Visconti
Martin Vuagnoux
Zhiguo Wan
Guilin Wang
Huaxiong Wang
Pan Wang
Ruizhong Wei
Mi Wen
Jian Weng
Christopher Wolf
Katsunari Yoshioka
Qinghua Zhang
Rui Zhang
Weiliang Zhao
Huafei Zhu

Table of Contents

Stream Ciphers

Symmetric Key Ciphers

Network Security

Cryptographic Applications

Secure Implementation

Signatures

Theory

Invited Talk

Security Applications

Provable Security

Protocols

Hashing and Message Authentication