Lecture Notes in Computer Science 5594

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

Colin Boyd Juan González Nieto (Eds.)

Information Security and Privacy

14th Australasian Conference, ACISP 2009
Brisbane, Australia, July 1-3, 2009
Proceedings

Springer

Volume Editors

Colin Boyd
Juan González Nieto
Queensland University of Technology
Information Security Institute
GPO Box 2434, Brisbane, QLD 4001, Australia
E-mail: {c.boyd, j.gonzaleznieto}@qut.edu.au

Library of Congress Control Number: 2009930749

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 3-642-02619-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-02619-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12707515 06/3180 5 4 3 2 1 0

Preface

The 2009 Australasian Conference on Information Security and Privacy was the 14th in an annual series that started in 1996. Over the years ACISP has grown from a relatively small conference with a large proportion of papers coming from Australia into a truly international conference with an established reputation. ACISP 2009 was held at Queensland University of Technology in Brisbane, during July 1–3, 2009.

This year there were 106 paper submissions and from those 30 papers were accepted for presentation, but one was subsequently withdrawn. Authors of accepted papers came from 17 countries and 4 continents, illustrating the international flavor of ACISP. We would like to extend our sincere thanks to all authors who submitted papers to ACISP 2009.

The contributed papers were supplemented by two invited talks from eminent researchers in information security. Basie von Solms (University of Johannesburg), currently President of IFIP, raised the question of how well dressed is the information security king. L. Jean Camp (Indiana University) talked about how to harden the network from the friend within. We are grateful to both of them for sharing their extensive knowledge and setting challenging questions for the ACISP 2009 delegates.

We were fortunate to have an energetic team of experts who formed the Program Committee. Their names may be found overleaf, and we thank them warmly for their considerable efforts. This team was helped by an even larger number of individuals who reviewed papers in their particular areas of expertise. A list of these names is also provided which we hope is complete. We would like to express our thanks to Springer for continuing to support the ACISP conference and for help in the conference proceedings production.

We are delighted to acknowledge the generous financial sponsorship of ACISP 2009 by the Research Network for a Secure Australia (funded by the Australian Research Council). The conference was hosted by the Information Security Institute at Queensland University of Technology, who provided first-class facilities and material support. The excellent Local Organizing Committee was led by the ACISP 2009 General Chair, Ed Dawson, with key contributions from Elizabeth Hansford and Christine Orme. We made use of the iChair electronic submission and reviewing software written by Thomas Baignères and Matthieu Finiasz at EPFL, LASEC.

July 2009

Colin Boyd
Juan González Nieto

Organization

General Chair

Ed Dawson	Queensland University of Technology, Australia

Program Co-chairs

Colin Boyd	Queensland University of Technology, Australia
Juan González Nieto	Queensland University of Technology, Australia

Program Committee

Michel Abdalla	École Normale Supérieure, France
Tuomas Aura	Microsoft Research, UK
Feng Bao	Institute for Infocomm Research, Singapore
Lynn Batten	Deakin University, Australia
Mike Burmester	Florida State University, USA
Andrew Clark	Queensland University of Technology, Australia
Marc Dacier	Symantec Research Labs Europe, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Alain Durand	Thomson, France
Pierre-Alain Fouque	Ecole Normale Supérieure, France
Steven Galbraith	Royal Holloway, UK
Dieter Gollman	Hamburg University of Technology, Germany
Maria Isabel González Vasco	Universidad Rey Juan Carlos, Spain
Kwangjo Kim	Information and Communication University, Korea
Lars Knudsen	Technical University of Denmark, Denmark
Pil Joong Lee	Pohang University of Science and Technology, Korea
Xuejia Lai	Shanghai Jiaotong University, China
Mark Manulis	TU Darmstadt, Germany
Chris Mitchell	Royal Holloway, UK
Atsuko Miyaji	JAIST, Japan
Paul Montague	DSTO, Australia
Yi Mu	University of Wollongong, Australia
Eiji Okamoto	Tsukuba University, Japan
Pascal Paillier	Gemalto, France
Kenny Paterson	Royal Holloway, UK
Josef Pieprzyk	Macquarie University, Australia

Matt Robshaw	Orange Labs, France
Carsten Rudolph	Fraunhofer SIT, Germany
Mark Ryan	University of Birmingham, UK
Rei Safavi-Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Ron Steinfeld	Macquarie University, Australia
Douglas Stinson	University of Waterloo, Canada
Willy Susilo	University of Wollongong, Australia
Jorge Villar	Universitat Politècnica de Catalunya, Spain
Huaxiong Wang	Nanyang Technological University, Singapore
Duncan Wong	University of Hong Kong, China

External Reviewers

Davide Alessio	Shaoquan Jiang	Agusti Solanas
Myrto Arapinis	Marc Joye	Rainer Steinwandt
Tomoyuki Asano	Stefan Katzenbeisser	Pairat Thorncharoensri
Mina Askari	Angelos Keromytis	Leonie Simpson
Man Ho Au	Sun Young Kim	Bo Qin
Julia Borghoff	Izuru Kitamura	Rolando Trujillo Rasua
Joo Yeon Cho	Divyan M. Konidala	Jae Woo Seo
Imsung Choi	Gregor Leander	Michal Sramka
Carlos Cid	Hyunrok Lee	Xiaorui Sun
Nico Doettling	Corrado Leita	Tomas Toft
Ming Duan	Benoit Libert	Olivier Thonnard
Dang Nguyen Duc	Xibin Lin	Sungmok Shin
Orr Dunkelman	Hans Loehr	Sren S. Thomsen
Sungwook Eom	Xianhui Lu	Damien Vergnaud
Martin Gagné	Yi Lu	Nguyen Vo
Praveen Gauravaram	Atefeh Mashatan	Zhongmei Wan
David Galindo	Toshihiko Matsuo	Hongjun Wu
Zheng Gong	Krystian Matusiewicz	Mu-En Wu
Choudary Gorantla	Jörn Müller-Quade	Jiang Wu
Fuchun Guo	Hyeran Mun	Qianhong Wu
Jian Guo	Kris Narayan	Wei Wu
Kyusuk Han	Kazuto Ogawa	Zhongming Wu
Francisco Rodríguez	Kazumasa Omote	Xiaokang Xiong
Henríquez	Hyewon Park	Yeon-Hyeong Yang
Matt Henricksen	Vijayakrishnan	Myunghan Yoo
Javier Herranz	Pasupathinathan	Kazuki Yoneyama
Jonathan Hoch	Axel Poschmann	Tsz Hon Yuen
Dennis Hofheinz	Angel L. Perez del Pozo	Greg Zaverucha
Qiong Huang	Thomas Plantard	Lei Zhang
Xinyi Huang	Siamak Shahandashti	Liangfeng Zhang
Tibor Jager	Ben Smyth	Huafei Zhu

Table of Contents

Invited Lecture

Network Security

Symmetric Key Encryption

Hash Functions

Invited Lecture

Public Key Cryptography

Protocols

Implementation