Lecture Notes in Computer Science 7372

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

Willy Susilo Yi Mu Jennifer Seberry (Eds.)

Information Security and Privacy

17th Australasian Conference, ACISP 2012
Wollongong, NSW, Australia, July 9-11, 2012
Proceedings

Springer

Volume Editors

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-31447-6 e-ISBN 978-3-642-31448-3
DOI 10.1007/978-3-642-31448-3
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012940392

CR Subject Classification (1998): K.6.5, E.3, D.4.6, E.4, J.1, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 17th Australasian Conference on Information Security and Privacy (ACISP 2012) was held at Wollongong, Australia, during July 9–11, 2012. The conference was sponsored by the Centre for Computer and Information Security of the University of Wollongong. 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 89 submissions, out of which the Program Committee selected 30 full papers and 5 short 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 some fundamental theory, cryptanalysis, message authentications, hash functions, public key cryptography, digital signatures, identity-based cryptography, attribute-based cryptography, lattice-based cryptography, lightweight cryptography and RFIDs. 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 work to the conference.

In addition to the contributed papers, the program included two invited talks. The invited speakers were Mihir Bellare (University of California, San Diego), with the topic "A Cryptographic Treatment of the Wiretap Channel" and Jorge Munilla (Universidad de Málaga, Spain), with the topic "Operating Principles of RFID Sysems and Attacks Related to the Location." 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 Xuhua Zhou from Shanghai Jiao Tong University, P.R. China, for the paper "A Generic Construction of Accountable Decryption and Its Applications."

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. A special thanks to the Publication Chair, Man Ho Au, who spent a tremendous amount of time for the success of the conference. We would also 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 General Chair, Jennifer Seberry, and the Organizing Committee for their excellent contribution to the conference.

July 2012

Willy Susilo
Yi Mu

Organization

General Chair

Jennifer Seberry	University of Wollongong, Australia

Program Chairs

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

Program Committee

Michel Abdalla	École Normale Supérieure, France
Joonsang Baek	Khalifa University, United Arab Emirates
Alex Biryukov	Université du Luxembourg, Luxembourg
Paulo Barreto	University of São Paulo, Brazil
Feng Bao	Institute for Infocomm Research, Singapore
Lynn Batten	Deakin University, Australia
Colin Boyd	Queensland University of Technology, Australia
Serdar Boztas	RMIT, Australia
Xiaofeng Chen	Xidian University, China
Nicolas T. Courtois	University College London, UK
Yvo Desmedt	University College London, UK
Orr Dunkelman	University of Haifa, Israel
Steven Galbraith	University of Auckland, New Zealand
Qiong Huang	South China Agricultural University, PR China
Xinyi Huang	Fujian Normal University, PR China
Apu Kapadia	Indiana University Bloomington, USA
Xuejia Lai	Shanghai Jiaotong University, China
Dong Hoon Lee	Electronics and Telecommunications Research Institute, Korea
Keith Martin	Royal Holloway, University of London, UK
Chris Mitchell	Royal Holloway, University of London, UK
Fabien Laguilaumie	UCBN and CNRS, LIP (Lyon), France
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Juan Gonzales Nieto	Queensland University of Technology, Australia
Miyako Ohkubo	National Institute of Information and Communications Technology, Japan
Claudio Orlandi	Bar-Ilan University, Israel
Udaya Parampalli	University of Melbourne, Australia

Josef Pieprzyk	Macquarie University, Australia
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
Tsuyoshi Takagi	Kyushu University, Japan
Vijay Varadharajan	Macquarie University, Australia
Kan Yasuda	NTT Corporation, Japan
Guilin Wang	University of Wollongong, Australia
Huaxiong Wang	Nanyang Technological University, Singapore
Duncan S. Wong	City University of Hong Kong, Hong Kong
Shouhuai Xu	University of Texas at San Antonio, USA
Guomin Yang	National University of Singapore, Singapore

Publication Chair

Man Ho Au	University of Wollongong, Australia

Organizing Committee

Fuchun Guo	University of Wollongong, Australia
Thomas Plantard	University of Wollongong, Australia
Reza Reyhanitabar	University of Wollongong, Australia

External Reviewers

Manal Adham	Matt Henricksen	Fagen Li
Yoshinori Aono	Javier Herranz	Jin Li
Myrto Arapinis	Mathias Herrmann	Shen Li
Gilad Asharov	Qiong Huang	Tieyan Li
Sergiu Bursuc	Hyoseung Kim	Kaitai Liang
Guilhem Castagnos	Kitak Kim	Hoon Wei Lim
Melissa Chase	Milyoung Kim	Richard Lindner
Yuan Chen	Aleksandar Kircanski	Zhen Liu
Kai-Yuen Cheong	Woo Kwon Koo	Jiqiang Lu
Koji Chida	Ozgul Kucuk	Weiliang Luo
Bernard Colbert	Lakshmi Kuppusamy	Shah Mahmood
Anupam Datta	Junzuo Lai	Cuauhtemoc Mancillas-Lopez
Angelo De Caro	Yee Wei Law	Pedro Maat Massolino
Wei Gao	Hoi Le	Seiichi Matsuda
Jian Guo	Kwangsu Lee	Kirill Morozov
Guillaume Hanrot	Peter Lee	Shishir Nagaraja
Takuya Hayashi	Gaëtan Leurent	

Prasad G. Naldurg
Ta Toan Khoa Nguyen
Shirin Nilizadeh
Ryo Nishimaki
Kazumasa Omote
Jong Hwan Park
Seunghwan Park
Geovandro Pereira
Duong Hieu Phan
Haifeng Qian
Hasan Qunoo
Kenneth Radke
Somindu C. Ramanna
Asha Rao
Arnab Roy
Moustafa Saleh
Sumanta Sarkar
Yu Sasaki
Roman Schlegel
Jae Hong Seo
Naoyuki Shinohara
Leonie Simpson
Dondong Sun
Li Sun
Katsuyuki Takashima
Xiao Tan
Keisuke Tanaka
Fei Tang
Ashraful Tuhin
Fenghe Wang
Lihua Wang
Yongzhuang Wei
Li Xu
Piyi Yang
Yanjiang Yang
Masaya Yasuda
Bin Zhang
Hui Zhang
Kehuan Zhang
Liangfeng Zhang
Mingwu Zhang
Rui Zhang
Yinghui Zhang
Yun Zhang
Qingji Zheng
Huafei Zhu
Youwen Zhu

Table of Contents

Fundamentals

Cryptanalysis

Message Authentication Codes and Hash Functions

Public Key Cryptography

Digital Signatures

Identity-Based and Attribute-Based Cryptography

Lattice-Based Cryptography

Lightweight Cryptography

Short Papers