Lecture Notes in Computer Science **9723**

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

More information about this series at http://www.springer.com/series/7410

Joseph K. Liu · Ron Steinfeld (Eds.)

Information Security and Privacy

21st Australasian Conference, ACISP 2016
Melbourne, VIC, Australia, July 4–6, 2016
Proceedings, Part II

Springer

Editors
Joseph K. Liu
Monash University
Melbourne, VIC
Australia

Ron Steinfeld
Monash University
Melbourne, VIC
Australia

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-40366-3 ISBN 978-3-319-40367-0 (eBook)
DOI 10.1007/978-3-319-40367-0

Library of Congress Control Number: 2015940421

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

This volume contains the papers presented at ACISP 2016: the 21st Australasian Conference on Information Security and Privacy held during July 4–6, 2016, in Melbourne.

This year we received a record high number of submissions: 176. Each submission was reviewed by an average of 2.9 Program Committee members. The committee decided to accept 52 full papers and eight short papers. In addition, we also included eight invited papers in order to widen the coverage to different areas of cyber security such as smart cities security and bitcoin security. We would like to extend our sincere thanks to all authors who submitted their papers to ACISP 2016.

The program included two excellent and informative keynote addresses. One of them was from Prof. Elisa Bertino, of Purdue University in the USA. Another was from Prof. Chris Mitchell, of Royal Holloway, University of London in the UK. Furthermore, our program also included eight invited talks from eight international well-known researchers in cyber security. They were Prof. Ed Dawson from Queensland University of Technology, Australia; Prof. Willy Susilo from University of Wollongong, Australia; Prof. Xun Yi from RMIT, Australia; Prof. Yu Yu from Shanghai Jiao Tong University, China; Prof. Wenlei Zhou from Deakin University, Australia; Dr. Surya Nepal from Data61, Australia; Prof. Jinjun Chen from University of Technology Sydney, Australia; and Dr. Jonathan Oliver from Trend Micro, Australia.

We would like to thank the 86 Program Committee members (from 22 different countries) as well as the external reviewers for their volunteer work of reading and discussing the submissions. We also deeply thank the general chair, Prof. Yang Xiang, publication co-chairs, Dr. Dong Seong Kim and Dr. Kaitai Liang, publicity chair, Dr. Nalin Asanka, and the Web chair, Dr. Yu Wang. This conference would not have been successful without their great assistance. Last but not least, we would like to thank EasyChair for providing a user-friendly interface for us to manage all submissions and proceeding files.

July 2016

Joseph K. Liu
Ron Steinfeld

Organization

Program Committee

Cristina Alcaraz	University of Malaga, Spain
Myrto Arapinis	University of Edinburgh, UK
Claudio Ardagna	Università degli Studi di Milano, Italy
David Aspinall	University of Edinburgh, UK
Giuseppe Ateniese	Sapienza University of Rome, Italy
Man Ho Au	Hong Kong Polytechnic University, HKSAR China
Joonsang Baek	Khalifa University of Science, Technology and Research, UAE
Zubair Baig	Edith Cowan University, Australia
Lynn Batten	Deakin University, Australia
Colin Boyd	Norwegian University of Science and Technology (NTNU), Norway
Serdar Boztas	RMIT University, Australia
Alvaro Cardenas	University of Texas at Dallas, USA
Aniello Castiglione	University of Salerno, Italy
Jinjun Chen	University of Technology Sydney, Australia
Liqun Chen	Hewlett-Packard Laboratories, UK
Xiaofeng Chen	Xidian University, China
Ray Cheung	City University of Hong Kong, HKSAR China
Kim-Kwang Raymond Choo	University of South Australia, Australia
Christophe Doche	Macquarie University, Australia
Ernest Foo	Queensland University of Technology, Australia
Steven Galbraith	Auckland University, New Zealand
David Galindo	SCYTL Secure Electronic Voting, Spain
Felix Gomez Marmol	NEC Laboratories Europe, Germany
Swee-Huay Heng	Multimedia University, Malaysia
Andreas Holzer	University of Toronto, Canada
Xinyi Huang	Fujian Normal University, China
Mitsugu Iwamoto	University of Electro-Communications, Japan
Sanjay Jha	University of New South Wales, Australia
Akinori Kawachi	The University of Tokushima, Japan
Dong Seong Kim	University of Canterbury, New Zealand
Howon Kim	Pusan National University, South Korea
Steve Kremer	Inria Nancy - Grand Est, France
Marina Krotofil	European Network for Cyber Security, The Netherlands

Noboru Kunihiro	The University of Tokyo, Japan
Miroslaw Kutylowski	Wroclaw University of Technology, Poland
Junzuo Lai	Jinan University, China
Gaëtan Leurent	Inria, France
Jin Li	Guangzhou University, China
Yingjiu Li	Singapore Management University, Singapore
Zhen Li	Institute for Infocomm Research, Singapore
Kaitai Liang	Aalto University, Finland
Joseph Liu	Monash University, Australia
Shengli Liu	Shanghai Jiao Tong University, China
Zhe Liu	University of Waterloo, Canada
Javier Lopez	University of Malaga, Spain
Jiqiang Lu	Institute for Infocomm Research, Singapore
Rongxing Lu	Nanyang Technological University, Singapore
Kazuhiko Minematsu	NEC Corporation, Japan
Chris Mitchell	Royal Holloway, University of London, UK
Yi Mu	University of Wollongong, Australia
Udaya Parampalli	The University of Melbourne, Australia
Mathias Payer	Purdue University, USA
Christian Payne	Murdoch University, Australia
Thomas Peyrin	Ingenico, Singapore
Josef Pieprzyk	Queensland University of Technology, Australia
Michalis Polychronakis	Columbia University, USA
Kui Ren	State University of New York at Buffalo, USA
Reza Reyhanitabar	NEC Laboratories Europe, Germany
Carsten Rudolph	Monash University, Australia
Sushmita Ruj	Indian Statistical Institute, India
Joerg Schwenk	Ruhr-Universität Bochum, Germany
Jun Shao	Zhejiang Gongshang University, China
Taeshik Shon	Ajou University, South Korea
Haya Shulman	Technische Universität Darmstadt, Germany
Anna Squicciarini	Penn State University, USA
Ron Steinfeld	Monash University, Australia
Chunhua Su	Osaka University, Japan
Willy Susilo	University of Wollongong, Australia
Shaohua Tang	South China University of Technology, China
Juan Tapiador	Universidad Carlos III de Madrid, Spain
Mahesh Tripunitara	University of Waterloo, Canada
Craig Valli	Edith Cowan University, Australia
Frederik Vercauteren	K.U. Leuven - ESAT/COSIC, Belgium
Triet D. Vo-Huu	Northeastern University, USA
Petros Wallden	The University of Edinburgh, UK
Cong Wang	City University of Hong Kong, HKSAR China
Yu Wang	Deakin University, Australia
Sheng Wen	Deakin University, Australia
Qianhong Wu	Beihang University, China

Guomin Yang	University of Wollongong, Australia
Yanjiang Yang	Huawei, Singapore
Wun-She Yap	Universiti Tunku Abdul Rahman, Malaysia
Xun Yi	RMIT University, Australia
Yong Yu	University of Electronic Science and Technology, China
Tsz-Hon Yuen	Huawei, Singapore
Aaram Yun	Ulsan National Institute of Science and Technology, South Korea

Additional Reviewers

Alamer, Ahmed
Aono, Yoshinori
Behnia, Rouzbeh
Boura, Christina
Chattopadhyay, Anupam
Chen, Wei
Cheng, Yao
Chin, Ji-Jian
Cui, Hui
Dai, Tianxiang
El Ioini, Nabil
Gaudenzi, Filippo
Ghodosi, Hossein
Ghosh, Satrajit
Gotfryd, Karol
Guasch, Sandra
Han, Shuai
Hanzlik, Lucjan
He, Kai
He, Shuangyu
Higo, Haruna
Hirano, Takato
Hongjun, Wu
Imine, Abdessamad
Jahan, Mosarrat
Javali, Chitra
Kim, Jun Young
Kluczniak, Kamil
Koshiba, Takeshi
Lauer, Sebastian
Li, Fagen
Liang, Zhi
Liu, Weiran
Liu, Ximeng
Luykx, Atul
Majcher, Krzysztof
Morozov, Kirill
Murphy, Sean
Myers, David
Nieto, Ana
Nishimaki, Ryo
Nuida, Koji
Peikert, Chris
Peters, Thomas
Rahman, Anisur
Reparaz, Oscar
Roenne, Peter
Saito, Teruo
Sakzad, Amin
Schneider, Thomas
Sengupta, Binanda
Seo, Hwajeong
Shani, Barak
Shibutani, Kyoji
Sinha Roy, Sujoy
Späth, Christopher
Sun, Li
Sun, Shifeng
Szepieniec, Alan
Tan, Hailun
Tan, Syhyuan
Tso, Raylin
Velichkov, Vesselin
Vivek, Srinivas
Vizár, Damian
Wang, Jianfeng

Wang, Qin
Wei, Xiaochao
Yau, Wei-Chuen
Ye, Jun
Yu, Xingjie
Yu, Zuoxia
Zhang, Lei
Zhao, Chuan
Zhao, Minghao
Zheng, Haibin
Zhong, Lin
Zhou, Xiuwen

Contents – Part II

Searchable Encryption

Broadcast Encryption

Mathematical Primitives

Symmetric Cipher

Short Papers-Mobile Security

Short Papers-Network Security

Short Papers-Pseudo Random/One-way Function

Contents – Part I

Social Network Security

Bitcoin Security

Statistical Privacy

Network Security

Smart City Security

Digital Forensics

Lightweight Security

Secure Batch Processing

Pseudo Random/One-way Function

Cloud Storage Security

Password/QR Code Security

Functional Encryption and Attribute-Based Cryptosystem