

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

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

© Springer International Publishing Switzerland 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

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
Swhee-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
Howan 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
Mirosław Kutylowski	Wrocław 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
Yanjiang Yang
Wun-She Yap
Xun Yi
Yong Yu

Tsz-Hon Yuen
Aaram Yun

University of Wollongong, Australia
Huawei, Singapore
Universiti Tunku Abdul Rahman, Malaysia
RMIT University, Australia
University of Electronic Science and Technology,
China
Huawei, Singapore
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
Koshiha, 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

Signature and Key Management

One-Round Strong Oblivious Signature-Based Envelope	3
<i>Rongmao Chen, Yi Mu, Willy Susilo, Guomin Yang, Fuchun Guo, and Mingwu Zhang</i>	
Proxy Signature with Revocation	21
<i>Shengmin Xu, Guomin Yang, Yi Mu, and Sha Ma</i>	
On the Relations Between Security Notions in Hierarchical Key Assignment Schemes for Dynamic Structures	37
<i>Arcangelo Castiglione, Alfredo De Santis, Barbara Masucci, Francesco Palmieri, and Aniello Castiglione</i>	

Public Key and Identity-Based Encryption

Content-Based Encryption	57
<i>Xiaofen Wang and Yi Mu</i>	
Provably Secure Threshold Paillier Encryption Based on Hyperplane Geometry	73
<i>Zhe Xia, Xiaoyun Yang, Min Xiao, and Debiao He</i>	
Identity-Based Group Encryption	87
<i>Xiling Luo, Yili Ren, Jingwen Liu, Jiankun Hu, Weiran Liu, Zhen Wang, Wei Xu, and Qianhong Wu</i>	
Edit Distance Based Encryption and Its Application	103
<i>Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, and Kaitai Liang</i>	
Proxy Re-encryption with Delegatable Verifiability	120
<i>Xiaodong Lin and Rongxing Lu</i>	
Efficient Completely Non-Malleable and RKA Secure Public Key Encryptions	134
<i>Shi-Feng Sun, Udaya Parampalli, Tsz Hon Yuen, Yu Yu, and Dawu Gu</i>	

Searchable Encryption

Verifiable Searchable Encryption with Aggregate Keys for Data Sharing in Outsourcing Storage	153
<i>Tong Li, Zheli Liu, Ping Li, Chunfu Jia, Zoe L. Jiang, and Jin Li</i>	
Public Key Encryption with Authorized Keyword Search.	170
<i>Peng Jiang, Yi Mu, Fuchun Guo, and Qiaoyan Wen</i>	
Linear Encryption with Keyword Search	187
<i>Shiwei Zhang, Guomin Yang, and Yi Mu</i>	

Broadcast Encryption

Generic Anonymous Identity-Based Broadcast Encryption with Chosen-Ciphertext Security	207
<i>Kai He, Jian Weng, Man Ho Au, Yijun Mao, and Robert H. Deng</i>	
Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing	223
<i>Jianchang Lai, Yi Mu, Fuchun Guo, Willy Susilo, and Rongmao Chen</i>	

Mathematical Primitives

Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs.	243
<i>Atsushi Takayasu and Noboru Kunihiro</i>	
A New Attack on Three Variants of the RSA Cryptosystem.	258
<i>Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien</i>	
Generalized Hardness Assumption for Self-bilinear Map with Auxiliary Information	269
<i>Takashi Yamakawa, Goichiro Hanaoka, and Noboru Kunihiro</i>	
Deterministic Encoding into Twisted Edwards Curves	285
<i>Wei Yu, Kunpeng Wang, Bao Li, Xiaoyang He, and Song Tian</i>	

Symmetric Cipher

Improved Rebound Attacks on AESQ: Core Permutation of CAESAR Candidate PAEQ.	301
<i>Nasour Bagheri, Florian Mendel, and Yu Sasaki</i>	
Efficient Beyond-Birthday-Bound-Secure Deterministic Authenticated Encryption with Minimal Stretch.	317
<i>Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel</i>	

Improved (related-key) Attacks on Round-Reduced KATAN-32/48/64 Based on the Extended Boomerang Framework	333
<i>Jiageng Chen, Je Sen Teh, Chunhua Su, Azman Samsudin, and Junbin Fang</i>	
Authenticated Encryption with Small Stretch (or, How to Accelerate AERO)	347
<i>Kazuhiko Minematsu</i>	
Impossible Differential Cryptanalysis of 14-Round Camellia-192	363
<i>Keting Jia and Ning Wang</i>	
Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA	379
<i>Ling Song, Zhangjie Huang, and Qianqian Yang</i>	
On the Security of the LAC Authenticated Encryption Algorithm	395
<i>Jiqiang Lu</i>	
Linear Hull Attack on Round-Reduced Simeck with Dynamic Key-Guessing Techniques	409
<i>Lingyue Qin, Huaifeng Chen, and Xiaoyun Wang</i>	
Short Papers-Public Key and Identity-Based Encryption	
Reducing the Key Size of the SRP Encryption Scheme	427
<i>Dung Hoang Duong, Albrecht Petzoldt, and Tsuyoshi Takagi</i>	
Short Papers-Biometric Security	
Biometric Access Control with High Dimensional Facial Features.	437
<i>Ying Han Pang, Ean Yee Khor, and Shih Yin Ooi</i>	
Security Analysis on Privacy-Preserving Cloud Aided Biometric Identification Schemes.	446
<i>Shiran Pan, Shen Yan, and Wen-Tao Zhu</i>	
Short Papers-Digital Forensics	
Interest Profiling for Security Monitoring and Forensic Investigation.	457
<i>Min Yang, Fei Xu, and Kam-Pui Chow</i>	
Short Papers-National Security Infrastructure	
Pseudonymous Signature on eIDAS Token – Implementation Based Privacy Threats.	467
<i>Miroslaw Kutylowski, Lucjan Hanzlik, and Kamil Kluczniak</i>	

Short Papers-Mobile Security

A Feasible No-Root Approach on Android. 481
Yao Cheng, Yingjiu Li, and Robert H. Deng

Short Papers-Network Security

Improved Classification of Known and Unknown Network Traffic Flows
Using Semi-supervised Machine Learning 493
Timothy Glennan, Christopher Leckie, and Sarah M. Erfani

Short Papers-Pseudo Random/One-way Function

A Noiseless Key-Homomorphic PRF: Application on Distributed Storage
Systems 505
Jhordany Rodriguez Parra, Terence Chan, and Siu-Wai Ho

Author Index 515

Contents – Part I

Invited Papers

I Know Where You All Are! Exploiting Mobile Social Apps for Large-Scale Location Privacy Probing	3
<i>Shuang Zhao, Xiapu Luo, Bo Bai, Xiaobo Ma, Wei Zou, Xinliang Qiu, and Man Ho Au</i>	
MUSE: Towards Robust and Stealthy Mobile Botnets via Multiple Message Push Services	20
<i>Wei Chen, Xiapu Luo, Chengyu Yin, Bin Xiao, Man Ho Au, and Yajuan Tang</i>	
A Survey on the Cyber Attacks Against Non-linear State Estimation in Smart Grids	40
<i>Jingxuan Wang, Lucas C.K. Hui, S.M. Yiu, Xingmin Cui, Eric Ke Wang, and Junbin Fang</i>	
Towards Bitcoin Payment Networks	57
<i>Patrick McCorry, Malte Möser, Siamak F. Shahandasti, and Feng Hao</i>	
Statistical Disclosure Control for Data Privacy Using Sequence of Generalised Linear Models	77
<i>Min Cherng Lee, Robin Mitra, Emmanuel Lazaridis, An Chow Lai, Yong Kheng Goh, and Wun-She Yap</i>	
Energy-Efficient Elliptic Curve Cryptography for MSP430-Based Wireless Sensor Nodes	94
<i>Zhe Liu, Johann Großschädl, Lin Li, and Qiuliang Xu</i>	

National Security Infrastructure

A Comparison Study of Wireless Network Security in Several Australasian Cities and Suburbs	115
<i>Alastair Nisbet and Andrew Woodward</i>	
On the Guessability of Resident Registration Numbers in South Korea	128
<i>Youngbae Song, Hyoungshick Kim, and Jun Ho Huh</i>	

Social Network Security

Towards Privacy-Preserving Data Mining in Online Social Networks: Distance-Grained and Item-Grained Differential Privacy.	141
<i>Shen Yan, Shiran Pan, Yuhang Zhao, and Wen-Tao Zhu</i>	

Bitcoin Security

Fair Client Puzzles from the Bitcoin Blockchain	161
<i>Colin Boyd and Christopher Carr</i>	

Statistical Privacy

Privacy-Preserving k -Nearest Neighbour Query on Outsourced Database	181
<i>Rui Xu, Kirill Morozov, Yanjiang Yang, Jianying Zhou, and Tsuyoshi Takagi</i>	
Reversible Data Hiding for Encrypted Images Based on Statistical Learning . . .	198
<i>Zhen Li and Wei Wu</i>	

Network Security

An Ensemble Learning Approach for Addressing the Class Imbalance Problem in Twitter Spam Detection.	215
<i>Shigang Liu, Yu Wang, Chao Chen, and Yang Xiang</i>	

Smart City Security

Putting the User in Control of the Intelligent Transportation System	231
<i>Catalin Gosman, Tudor Cornea, Ciprian Dobre, Florin Pop, and Aniello Castiglione</i>	

Digital Forensics

Exploring the Space of Digital Evidence – Position Paper	249
<i>Carsten Rudolph</i>	

Lightweight Security

Towards Lightweight Anonymous Entity Authentication for IoT Applications.	265
<i>Yanjiang Yang, Haibin Cai, Zhuo Wei, Haibing Lu, and Kim-Kwang Raymond Choo</i>	
Hybrid MQ Signature for Embedded Device	281
<i>Shaohua Tang, Bo Lv, and Wuqiang Shen</i>	

Secure Batch Processing

Batch Verifiable Computation with Public Verifiability for Outsourcing Polynomials and Matrix Computations.	293
<i>Yujuan Sun, Yu Yu, Xiangxue Li, Kai Zhang, Haifeng Qian, and Yuan Zhou</i>	
Accelerating Oblivious Transfer with Batch Multi-exponentiation	310
<i>Yang Sun, Qianhong Wu, Jingwen Liu, Jianwei Liu, Xinyi Huang, Bo Qin, and Wei Hu</i>	

Pseudo Random/One-way Function

CTM-sp: A Family of Cryptographic Hash Functions from Chaotic Tent Maps.	329
<i>Xun Yi, Xuechao Yang, Yong Feng, Fengling Han, and Ron van Schyndel</i>	
One-Key Compression Function Based MAC with Security Beyond Birthday Bound	343
<i>Avijit Dutta, Mridul Nandi, and Goutam Paul</i>	

Cloud Storage Security

Towards Efficient Fully Randomized Message-Locked Encryption	361
<i>Tao Jiang, Xiaofeng Chen, Qianhong Wu, Jianfeng Ma, Willy Susilo, and Wenjing Lou</i>	
Secure and Traceable Framework for Data Circulation.	376
<i>Kaitai Liang, Atsuko Miyaji, and Chunhua Su</i>	
Public Cloud Data Auditing with Practical Key Update and Zero Knowledge Privacy	389
<i>Yong Yu, Yannan Li, Man Ho Au, Willy Susilo, Kim-Kwang Raymond Choo, and Xinpeng Zhang</i>	

Password/QR Code Security

Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing	409
<i>Yang-Wai Chow, Willy Susilo, Guomin Yang, James G. Phillips, Ilung Pranata, and Ari Moesriami Barmawi</i>	
Password Requirements Markup Language.	426
<i>Moritz Horsch, Mario Schlipf, Johannes Braun, and Johannes Buchmann</i>	

Functional Encryption and Attribute-Based Cryptosystem

Leakage-Resilient Functional Encryption via Pair Encodings	443
<i>Zuoxia Yu, Man Ho Au, Qiuliang Xu, Rupeng Yang, and Jinguang Han</i>	
Secret Handshakes with Dynamic Expressive Matching Policy	461
<i>Lin Hou, Junzuo Lai, and Lixian Liu</i>	
Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance	477
<i>Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo</i>	
Chosen Ciphertext Secure Attribute-Based Encryption with Outsourced Decryption	495
<i>Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji</i>	
Accountable Large-Universe Attribute-Based Encryption Supporting Any Monotone Access Structures.	509
<i>Yinghui Zhang, Jin Li, Dong Zheng, Xiaofeng Chen, and Hui Li</i>	
A Cloud-Based Access Control Scheme with User Revocation and Attribute Update	525
<i>Peng Zhang, Zehong Chen, Kaitai Liang, Shulan Wang, and Ting Wang</i>	
Author Index	541