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
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 Krotofi 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
Kazuhiro 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  
Liu, Ximeng

Aono, Yoshinori  
Luykx, Atul

Behnia, Rouzbeh  
Majcher, Krzysztof

Boura, Christina  
Morozov, Kirill

Chattopadhyay, Anupam  
Murphy, Sean

Chen, Wei  
Myers, David

Cheng, Yao  
Nieto, Ana

Chin, Ji-Jian  
Nishimaki, Ryo

Cui, Hui  
Nuida, Koji

Dai, Tianxiang  
Peikert, Chris

El Ioini, Nabil  
Peters, Thomas

Gaudenzi, Filippo  
Rahman, Anisur

Ghodosi, Hossein  
Reparaz, Oscar

Ghosh, Satrajit  
Roenne, Peter

Gottfryd, Karol  
Saito, Teruo

Guasch, Sandra  
Sakzad, Amin

Han, Shuai  
Schneider, Thomas

Hanzlik, Lucjan  
Sengupta, Binanda

He, Kai  
Seo, Hwajeong

He, Shuangyu  
Shani, Barak

Higo, Haruna  
Shibutani, Kyoji

Hirano, Takato  
Sinha Roy, Sujoy

Hongjun, Wu  
Späth, Christopher

Imine, Abdessamad  
Sun, Li

Jahan, Mosarrat  
Sun, Shifeng

Javali, Chitra  
Szepieniec, Alan

Kim, Jun Young  
Tan, Hailun

Kluczniai, Kamil  
Tan, Syhyuan

Koshiba, Takeshi  
Tso, Raylin

Lauer, Sebastian  
Velichkov, Vesselin

Li, Fagen  
Vivek, Srinivas

Liang, Zhi  
Vizár, Damian

Liu, Weiran  
Wang, Jianfeng
<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wang, Qin</td>
<td>Zhang, Lei</td>
</tr>
<tr>
<td>Wei, Xiaochao</td>
<td>Zhao, Chuan</td>
</tr>
<tr>
<td>Yau, Wei-Chuen</td>
<td>Zhao, Minghao</td>
</tr>
<tr>
<td>Ye, Jun</td>
<td>Zheng, Haibin</td>
</tr>
<tr>
<td>Yu, Xingjie</td>
<td>Zhong, Lin</td>
</tr>
<tr>
<td>Yu, Zuoxia</td>
<td>Zhou, Xiuwen</td>
</tr>
</tbody>
</table>
Contents – Part I

Invited Papers

I Know Where You All Are! Exploiting Mobile Social Apps for Large-Scale Location Privacy Probing ................................................. 3
  Shuang Zhao, Xiapu Luo, Bo Bai, Xiaobo Ma, Wei Zou, Xinliang Qiu, and Man Ho Au

MUSE: Towards Robust and Stealthy Mobile Botnets via Multiple Message Push Services ............................................................. 20
  Wei Chen, Xiapu Luo, Chengyu Yin, Bin Xiao, Man Ho Au, and Yajuan Tang

A Survey on the Cyber Attacks Against Non-linear State Estimation in Smart Grids ........................................................................... 40
  Jingxuan Wang, Lucas C.K. Hui, S.M. Yiu, Xingmin Cui, Eric Ke Wang, and Junbin Fang

Towards Bitcoin Payment Networks ............................................................. 57
  Patrick McCorry, Malte Möser, Siamak F. Shahandasti, and Feng Hao

Statistical Disclosure Control for Data Privacy Using Sequence of Generalised Linear Models ......................................................... 77
  Min Cherng Lee, Robin Mitra, Emmanuel Lazaridis, An Chow Lai, Yong Kheng Goh, and Wun-She Yap

Energy-Efficient Elliptic Curve Cryptography for MSP430-Based Wireless Sensor Nodes ......................................................... 94
  Zhe Liu, Johann Großschäd, Lin Li, and Qiuliang Xu

National Security Infrastructure

A Comparison Study of Wireless Network Security in Several Australasian Cities and Suburbs ......................................................... 115
  Alastair Nisbet and Andrew Woodward

On the Guessability of Resident Registration Numbers in South Korea ...... 128
  Youngbae Song, Hyoungshick Kim, and Jun Ho Huh
Social Network Security

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

Bitcoin Security

Fair Client Puzzles from the Bitcoin Blockchain ......................... 161
Colin Boyd and Christopher Carr

Statistical Privacy

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

Network Security

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

Smart City Security

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

Digital Forensics

Exploring the Space of Digital Evidence – Position Paper ................. 249
Carsten Rudolph

Lightweight Security

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

Batch Verifiable Computation with Public Verifiability for Outsourcing
Polynomials and Matrix Computations .......................... 293
  Yujuan Sun, Yu Yu, Xiangxue Li, Kai Zhang, Haifeng Qian,
  and Yuan Zhou

Accelerating Oblivious Transfer with Batch Multi-exponentiation ...... 310
  Yang Sun, Qianhong Wu, Jingwen Liu, Jianwei Liu, Xinyi Huang,
  Bo Qin, and Wei Hu

Pseudo Random/One-way Function

CTM-sp: A Family of Cryptographic Hash Functions from Chaotic Tent
Maps ................................................................. 329
  Xun Yi, Xuechao Yang, Yong Feng, Fengling Han,
  and Ron van Schyndel

One-Key Compression Function Based MAC with Security Beyond
Birthday Bound ......................................................... 343
  Avijit Dutta, Mridul Nandi, and Goutam Paul

Cloud Storage Security

Towards Efficient Fully Randomized Message-Locked Encryption ........ 361
  Tao Jiang, Xiaofeng Chen, Qianhong Wu, Jianfeng Ma, Willy Susilo,
  and Wenjing Lou

Secure and Traceable Framework for Data Circulation..................... 376
  Kaitai Liang, Atsuko Miyaji, and Chunhua Su

Public Cloud Data Auditing with Practical Key Update and Zero
Knowledge Privacy ..................................................... 389
  Yong Yu, Yannan Li, Man Ho Au, Willy Susilo,
  Kim-Kwang Raymond Choo, and Xinpeng Zhang

Password/QR Code Security

Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing .... 409
  Yang-Wai Chow, Willy Susilo, Guomin Yang, James G. Phillips,
  Ilung Pranata, and Ari Moesriami Barmawi

Password Requirements Markup Language ............................. 426
  Moritz Horsch, Mario Schlipf, Johannes Braun,
  and Johannes Buchmann
Functional Encryption and Attribute-Based Cryptosystem

Leakage-Resilient Functional Encryption via Pair Encodings .................................. 443
   Zuoxia Yu, Man Ho Au, Qiuliang Xu, Rupeng Yang, and Jinguang Han

Secret Handshakes with Dynamic Expressive Matching Policy ................................. 461
   Lin Hou, Junzuo Lai, and Lixian Liu

Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance .......................................................... 477
   Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo

Chosen Ciphertext Secure Attribute-Based Encryption with Outsourced Decryption .......................................................... 495
   Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji

Accountable Large-Universe Attribute-Based Encryption Supporting Any Monotone Access Structures ............................................ 509
   Yinghui Zhang, Jin Li, Dong Zheng, Xiaofeng Chen, and Hui Li

A Cloud-Based Access Control Scheme with User Revocation and Attribute Update .......................................................... 525
   Peng Zhang, Zehong Chen, Kaitai Liang, Shulan Wang, and Ting Wang

Author Index .................................................................................................................. 541
Contents – Part II

Signature and Key Management

One-Round Strong Oblivious Signature-Based Envelope ................................. 3
   Rongmao Chen, Yi Mu, Willy Susilo, Guomin Yang, Fuchun Guo,
   and Mingwu Zhang

Proxy Signature with Revocation ................................................................. 21
   Shengmin Xu, Guomin Yang, Yi Mu, and Sha Ma

On the Relations Between Security Notions in Hierarchical Key
Assignment Schemes for Dynamic Structures ............................................. 37
   Arcangelo Castiglione, Alfredo De Santis, Barbara Masucci,
   Francesco Palmieri, and Aniello Castiglione

Public Key and Identity-Based Encryption

Content-Based Encryption ................................................................. 57
   Xiaofen Wang and Yi Mu

Provably Secure Threshold Paillier Encryption Based on Hyperplane
Geometry ........................................................................................................ 73
   Zhe Xia, Xiaoyun Yang, Min Xiao, and Debiao He

Identity-Based Group Encryption ................................................................. 87
   Xiling Luo, Yili Ren, Jingwen Liu, Jiankun Hu, Weiran Liu,
   Zhen Wang, Wei Xu, and Qianhong Wu

Edit Distance Based Encryption and Its Application ................................. 103
   Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, and Kaitai Liang

Proxy Re-encryption with Delegatable Verifiability ..................................... 120
   Xiaodong Lin and Rongxing Lu

Efficient Completely Non-Malleable and RKA Secure Public Key
Encryptions .................................................................................................... 134
   Shi-Feng Sun, Udaya Parampalli, Tsz Hon Yuen, Yu Yu, and Dawu Gu
Searchable Encryption

Verifiable Searchable Encryption with Aggregate Keys for Data Sharing in Outsourcing Storage ........................................... 153
   Tong Li, Zheli Liu, Ping Li, Chunfu Jia, Zoe L. Jiang, and Jin Li

Public Key Encryption with Authorized Keyword Search ................. 170
   Peng Jiang, Yi Mu, Fuchun Guo, and Qiaoyan Wen

Linear Encryption with Keyword Search ..................................... 187
   Shiwei Zhang, Guomin Yang, and Yi Mu

Broadcast Encryption

Generic Anonymous Identity-Based Broadcast Encryption
with Chosen-Ciphertext Security ............................................. 207
   Kai He, Jian Weng, Man Ho Au, Yijun Mao, and Robert H. Deng

Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing ..................................................... 223
   Jianchang Lai, Yi Mu, Fuchun Guo, Willy Susilo, and Rongmao Chen

Mathematical Primitives

Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs ...... 243
   Atsushi Takayasu and Noboru Kunihiro

A New Attack on Three Variants of the RSA Cryptosystem ................. 258
   Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien

Generalized Hardness Assumption for Self-bilinear Map with Auxiliary Information ..................................................... 269
   Takashi Yamakawa, Goichiro Hanaoka, and Noboru Kunihiro

Deterministic Encoding into Twisted Edwards Curves ....................... 285
   Wei Yu, Kunpeng Wang, Bao Li, Xiaoyang He, and Song Tian

Symmetric Cipher

Improved Rebound Attacks on AESQ: Core Permutation of CAESAR Candidate PAEQ ....................................................... 301
   Nasour Bagheri, Florian Mendel, and Yu Sasaki

Efficient Beyond-Birthday-Bound-Secure Deterministic Authenticated Encryption with Minimal Stretch ............................. 317
   Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel
Improved (related-key) Attacks on Round-Reduced KATAN-32/48/64
Based on the Extended Boomerang Framework .............................................. 333
    Jiageng Chen, Je Sen Teh, Chunhua Su, Azman Samsudin,
    and Junbin Fang

Authenticated Encryption with Small Stretch (or, How to Accelerate
AERO) ............................................................................................................. 347
    Kazuhiko Minematsu

Impossible Differential Cryptanalysis of 14-Round Camellia-192 ............... 363
    Keting Jia and Ning Wang

Automatic Differential Analysis of ARX Block Ciphers with Application to
SPECK and LEA ............................................................................................. 379
    Ling Song, Zhangjie Huang, and Qianqian Yang

On the Security of the LAC Authenticated Encryption Algorithm ............ 395
    Jiqiang Lu

Linear Hull Attack on Round-Reduced Simeck with Dynamic
Key-Guessing Techniques ............................................................................. 409
    Lingyue Qin, Huaiwen Chen, and Xiaoyun Wang

Short Papers-Public Key and Identity-Based Encryption

Reducing the Key Size of the SRP Encryption Scheme .............................. 427
    Dung Hoang Duong, Albrecht Petzoldt, and Tsuyoshi Takagi

Short Papers-Biometric Security

Biometric Access Control with High Dimensional Facial Features ............. 437
    Ying Han Pang, Ean Yee Khor, and Shih Yin Ooi

Security Analysis on Privacy-Preserving Cloud Aided Biometric
Identification Schemes .................................................................................. 446
    Shiran Pan, Shen Yan, and Wen-Tao Zhu

Short Papers-Digital Forensics

Interest Profiling for Security Monitoring and Forensic Investigation .......... 457
    Min Yang, Fei Xu, and Kam-Pui Chow

Short Papers-National Security Infrastructure

Pseudonymous Signature on eIDAS Token – Implementation Based
Privacy Threats ............................................................................................... 467
    Mirosław Kutylowski, Lucjan Hanzlik, and Kamil Klucznik
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