

Communications in Computer and Information Science

651

Commenced Publication in 2007

Founding and Former Series Editors:

Alfredo Cuzzocrea, Dominik Ślęzak, and Xiaokang Yang

Editorial Board

Simone Diniz Junqueira Barbosa

*Pontifical Catholic University of Rio de Janeiro (PUC-Rio),
Rio de Janeiro, Brazil*

Phoebe Chen

La Trobe University, Melbourne, Australia

Xiaoyong Du

Renmin University of China, Beijing, China

Joaquim Filipe

Polytechnic Institute of Setúbal, Setúbal, Portugal

Orhun Kara

TÜBİTAK BİLGEM and Middle East Technical University, Ankara, Turkey

Igor Kotenko

*St. Petersburg Institute for Informatics and Automation of the Russian
Academy of Sciences, St. Petersburg, Russia*

Ting Liu

Harbin Institute of Technology (HIT), Harbin, China

Krishna M. Sivalingam

Indian Institute of Technology Madras, Chennai, India

Takashi Washio

Osaka University, Osaka, Japan

More information about this series at <http://www.springer.com/series/7899>

Lynn Batten · Gang Li (Eds.)

Applications and Techniques in Information Security

6th International Conference, ATIS 2016
Cairns, QLD, Australia, October 26–28, 2016
Proceedings

Editors

Lynn Batten
School of Information Technology
Deakin University
Geelong
Australia

Gang Li
School of Information Technology
Deakin University
Geelong
Australia

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-981-10-2740-6 ISBN 978-981-10-2741-3 (eBook)
DOI 10.1007/978-981-10-2741-3

Library of Congress Control Number: 2016953327

© Springer Nature Singapore Pte Ltd. 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 Nature Singapore Pte Ltd.

The registered company address is: 152 Beach Road, #22-06/08 Gateway East, Singapore 189721, Singapore

Preface

The International Conference on Applications and Techniques in Information Security (ATIS) has been held annually since 2010. This year, the seventh in the series was held at Central Queensland University, Cairns, Australia, during October 26–28, 2016. ATIS 2016 focuses on all aspects of techniques and applications in information security research, and provides a valuable connection between the theoretical and the implementation communities attracting participants from industry, academia, and government organizations.

The selection process this year was competitive, each submitted paper was reviewed by three members of the Program Committee. Following this independent review, there were discussions among reviewers and chairs. A total of ten papers were selected as full papers, and another three papers were selected as short papers.

We would like to thank everyone who participated in the development of the ATIS 2016 program. In particular, we would give special thanks to the Program Committee, for their diligence and concern for the quality of the program, and also with their detailed feedback to the authors. The general organization of the conference also relied on the efforts of ATIS 2016 Organizing Committee. We especially thank Biplob Ray, Judy Chow, and Gina Jing for the general administrative issues, the registration process, and the maintaining of the conference website.

Finally and most importantly, we thank all the authors, who are the primary reason why ATIS 2016 is so exciting, and why it is the premier forum for presentation and discussion of innovative ideas, research results, applications, and experience from around the world as well as for highlight activities in the related areas. Because of your great work, ATIS 2016 was a great success.

September 2016

Lynn Batten
Gang Li

Organization

ATIS 2016 was organized by the School of Engineering and Technology, Central Queensland University (Australia), and the School of Information Technology, Deakin University (Australia).

ATIS 2016 Steering Committee

Steering Committee

Lynn Batten (Chair)	Deakin University, Australia
Heejo Lee	Korea University, Korea
Gang Li (Secretary)	Deakin University, Australia
Jiqiang Liu	Beijing Jiaotong University, China
Tsutomu Matsumoto	Yokohama National University, Japan
Wenjia Niu	Chinese Academy of Sciences, China
Yuliang Zheng	University of Alabama at Birmingham, USA

ATIS 2016 Organizing Committee

Program Co-chairs

Lynn Batten	Deakin University, Australia
Gang Li	Deakin University, Australia

Conference Advisor

William Guo	Central Queensland University, Australia
-------------	--

Organizing Committee

Biplob Ray (Chair)	Central Queensland University, Australia
Rudd Rankine	Central Queensland University, Australia
Nur Hussan	Central Queensland University, Australia
Joy Jenkins	Central Queensland University, Australia
Gina Jing (Secretary)	Central Queensland University, Australia
Jamie Shield	Central Queensland University, Australia

ATIS 2016 Program Committee

Mamoun Alazab	Macquarie University, Australia
Moutaz Alazab	Melbourne Institute of Technology, Australia
Edilson Arenas	Central Queensland University, Australia
Leijla Batina	Radboud University, The Netherlands
Liang Chang	University of Manchester, UK
Guoyong Cai	Guilin University of Electronic Technology, China
Morshed Choudhury	Deakin University, Australia

Xuejie Ding	Chinese Academy of Sciences, China
Jiaxin Han	Xi'an Shiyong University, China
Nur Hussan	Central Queensland University, Australia
Meena Jha	Central Queensland University, Australia
Rafiqul Islam	Charles Sturt University, Australia
Kwangjo Kim	KAIST, Korea
Jie Kong	Xi'an Shiyong University, China
Heejo Lee	Korea University, Korea
Qingyun Liu	Chinese Academy of Sciences, China
Yufeng Lin	Central Queensland University, Australia
Jiqiang Liu	Beijing Jiaotong University, China
Wei Ma	Chinese Academy of Sciences, China
Lei Pan	Deakin University, Australia
Na Pang	Chinese Academy of Sciences, China
Rudd Rankin	Central Queensland University, Australia
Biplob Ray	Central Queensland University, Australia
Wei Ren	China University of Geosciences, China
Zhongzhi Shi	Chinese Academy of Sciences, China
Tony de Souza-Daw	Melbourne Polytechnic, Australia
Lisa Soon	Central Queensland University, Australia
Jamie Shield	Central Queensland University, Australia
Jinqiao Shi	Chinese Academy of Sciences, China
Dirk Thatmann	Technische Universitaet Berlin, Germany
Steve Versteeg	CA, Australia
Matthew Warren	Deakin University, Australia
Xiaofeng Wang	Siemens Research, China
Hongtao Wang	Chinese Academy of Sciences, China
Ping Xiong	Zhongnan University of Economic, China
Gang Xiong	Chinese Academy of Sciences, China
Rui Xue	Chinese Academy of Sciences, China
Fei Yan	Wuhan University, China
Ziqi Yan	Beijing Jiaotong University, China
Feng Yi	Chinese Academy of Sciences, China
Xun Yi	RMIT University, Australia
John Yearwood	Deakin University, Australia
Chengde Zhang	Southwest Jiaotong University, China
Yuan Zhang	Nanjing University, China
Dali Zhu	Chinese Academy of Sciences, China
Liehuang Zhu	Beijing Institute of Technology, China
Tianqing Zhu	Deakin University, Australia
Tingshao Zhu	Chinese Academy of Sciences, China
Yujia Zhu	Chinese Academy of Sciences, China

Sponsoring Institutions

Central Queensland University, Australia

Deakin University, Australia

Invited Speeches

Countermeasures Against Implementation Attacks on Private and Public-Key Cryptosystems

Paolo Maistri

Centre National De Ra Recherche Scientifique, Paris, France
`paolo.maistri@imag.fr`

Abstract. Implementing a secure system is much more complex than providing a theoretically secure algorithm. Careless implementations can be easily vulnerable to a large spectrum of passive and/or active attacks. In this talk, we will present the most important attacks and a (non- exhaustive) list of possible countermeasures that will make the attacker's job a bit harder. Both symmetric and asymmetric cryptography will be presented, with application examples to the Advanced Encryption Standard and Elliptic Curve Cryptosystems.

Keywords: Implementation attacks · Cryptography

Current and Emerging Issues in Privacy and Data Security in Queensland, Australia and Internationally

Philip Green

Office of the Information Commissioner, Brisbane City, QLD, Australia
Philip.Green@oic.qld.gov.au

Abstract. The increasing pace of technology and the explosion in production and collection of data has created serious challenges for privacy and data protection. Australia's privacy legislation dates back to 1988 and is largely based on international human rights protections that pre date this legislation. Where hacktivists or sophisticated hackers can mount attacks in a matter of days or weeks, government legislators and regulators and procurement processes can often take years to respond. Queensland's legislation is currently under review but even since 2009 has not kept up with the technological advances to date nor is it equipped to deal with the challenges of the future. The Panama leak has been used to argue that a kind of Moore's law applies to the magnitude of data breaches. Governments around the world have taken note and there is international debate on where lines should be drawn and the balance between privacy and security should be struck. Increasingly jurisdictions are investigating mandatory data breach notification and debating proportionality in terms of counter terrorism, privacy and other civil rights and ethical issues. Business and Government are looking for productivity gains and customer focused solutions to be had from big data and data analytics. Queensland's Privacy Commissioner will discuss emerging issues in privacy and data protection in Australia, the Queensland State and Internationally. In an increasingly connected and wired world, the challenges cannot be ignored and the stakes are high. Data security becomes of life threatening proportions in a virtual operating theatre or in a world of autonomous vehicles which is rapidly approaching.

Keywords: Data protection • Privacy

Contents

Attacks on Data Security Systems

A New Sign-Change Attack on the Montgomery Ladders	3
<i>Lynn Margaret Batten and Mohammed Khalil Amain</i>	
Investigating Cube Attacks on the Authenticated Encryption Stream Cipher ACORN.	15
<i>Md Iftekhar Salam, Harry Bartlett, Ed Dawson, Josef Pieprzyk, Leonie Simpson, and Kenneth Koon-Ho Wong</i>	

Detection of Attacks on Data Security Systems

Investigating Security Vulnerabilities in Modern Vehicle Systems	29
<i>Xi Zheng, Lei Pan, Hongxu Chen, and Peiyin Wang</i>	
Tweaking Generic OTR to Avoid Forgery Attacks	41
<i>Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, and Kenneth Koon-Ho Wong</i>	
Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview	54
<i>Abdullahi Chowdhury</i>	

Data Security

Evaluating Entropy Sources for True Random Number Generators by Collision Counting	69
<i>Maciej Skórski</i>	
Enhancement of Sensor Data Transmission by Inference and Efficient Data Processing	81
<i>James Jin Kang, Tom H. Luan, and Henry Larkin</i>	
An Improved EllipticNet Algorithm for Tate Pairing on Weierstrass’ Curves, Faster Point Arithmetic and Pairing on Selmer Curves and a Note on Double Scalar Multiplication	93
<i>Srinivasa Rao Subramanya Rao</i>	
Inductive Hierarchical Identity Based Key Agreement with Pre-deployment Interactions (i-H-IB-KA-pdi).	106
<i>Pinaki Sarkar and Morshed Uddin Chowdhury</i>	

Data Privacy

Identity-Based Threshold Encryption on Lattices with Application to Searchable Encryption	117
<i>Veronika Kuchta and Olivier Markowitch</i>	
Recursive M-ORAM: A Matrix ORAM for Clients with Constrained Storage Space	130
<i>Karin Sumongkayothin, Steven Gordon, Atsuko Miyaji, Chunhua Su, and Komwut Wipusitwarakun</i>	
False Signal Injection Attack Detection of Cyber Physical Systems by Event-Triggered Distributed Filtering over Sensor Networks	142
<i>Yufeng Lin, Biplob Ray, Dennis Jarvis, and Jia Wang</i>	
Mobile Money in the Australasian Region - A Technical Security Perspective	154
<i>Swathi Parasa and Lynn Margaret Batten</i>	
Author Index	163