

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, Zurich, 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 · Pierangela Samarati (Eds.)

Information Security Practice and Experience

13th International Conference, ISPEC 2017
Melbourne, VIC, Australia, December 13–15, 2017
Proceedings

Editors

Joseph K. Liu
Monash University
Clayton, VIC
Australia

Pierangela Samarati
University of Milan
Milan
Italy

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-72358-7

ISBN 978-3-319-72359-4 (eBook)

<https://doi.org/10.1007/978-3-319-72359-4>

Library of Congress Control Number: 2017960876

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers presented at ISPEC 2017: the 13th International Conference on Information Security Practice and Experience held during December 13–15, 2017 in Melbourne, Australia.

In response to the call for papers, 105 submissions were received. Submissions were evaluated on the basis of their significance, novelty, and technical quality, with an average of three reviews per paper. Based on the review and the Program Committee discussions, 34 full and 14 short papers were accepted. The program also includes nine papers from the SocialSec (3rd International Symposium on Security and Privacy in Social Networks and Big Data) Track.

We would like to express our thanks to all Program Committee members. Without their hard effort in reviewing papers in such a short time, the conference would not have been successful. We would also like to thank our general co-chairs, Prof. Robert Deng, Prof. Yang Xiang, and Prof. Wanlei Zhou, and our publicity chair, Dr. Yu Wang. They all devoted a large amount of time for the preparation of this conference.

Finally we would like to thank our sponsor, Huawei, for their continuing support of this conference!

December 2017

Joseph K. Liu
Pierangela Samarati

Organization

Program Committee

Man Ho Au	Hong Kong Polytechnic University, Hong Kong, SAR China
Joonsang Baek	University of Wollongong, Australia
Zubair Baig	Edith Cowan University, Australia
Carlo Blundo	Università degli Studi di Salerno, Italy
Colin Boyd	Norwegian University of Science and Technology, Norway
Alvaro Cardenas	University of Texas at Dallas, USA
Aniello Castiglione	University of Salerno, Italy
Jinjun Chen	University of Technology Sydney, Australia
Liqun Chen	University of Surrey, UK
Xiaofeng Chen	Xidian University, China
Raymond Choo	University of Texas at San Antonio, USA
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Sara Foresti	Università degli Studi di Milano, Italy
Angelo Genovese	Università degli Studi di Milano, Italy
Dieter Gollmann	Hamburg University of Technology, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Andreas Holzer	University of Toronto, Canada
Xinyi Huang	Fujian Normal University, China
Mitsugu Iwamoto	University of Electro-Communications, Japan
Julian Jang-Jaccard	Massey University, New Zealand
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Ryan Ko	University of Waikato, New Zealand
Noboru Kunihiro	The University of Tokyo, Japan
Mirosław Kutyłowski	Wrocław University of Technology, Poland
Junzuo Lai	Jinan University, China
Costas Lambrinoudakis	University of Piraeus, Greece
Albert Levi	Sabancı University, Turkey
Li Li	University of Luxembourg, Luxembourg
Ming Li	University of Arizona, USA
Kaitai Liang	Manchester Metropolitan University, UK
Joseph Liu	Monash University, Australia
Shengli Liu	Shanghai Jiao Tong University, China
Zhe Liu	University of Luxembourg, Luxembourg
Giovanni Livraga	Università degli Studi di Milano, Italy

Javier Lopez	University of Malaga, Spain
Jiqiang Lu	Institute for Infocomm Research, Singapore
Rongxing Lu	University of New Brunswick, Canada
Chris Mitchell	Royal Holloway, University of London, UK
Yi Mu	University of Wollongong, Australia
Josef Pieprzyk	Queensland University of Technology, Australia
Sushmita Ruj	Indian Statistical Institute, India
Pierangela Samarati	Università degli Studi di Milano, Italy
Jun Shao	Zhejiang Gongshang University, China
Taeshik Shon	Ajou University, South Korea
Ron Steinfeld	Monash University, Australia
Chunhua Su	University of Aizu, Japan
Willy Susilo	University of Wollongong, Australia
Cong Wang	City University of Hong Kong, SAR China
Ding Wang	Peking University, China
Guilin Wang	Huawei Singapore, Singapore
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, Singapore
Wun-She Yap	Universiti Tunku Abdul Rahman, Malaysia
Masaya Yasuda	Kyushu University, Japan
Jiangshan Yu	University of Luxembourg, Luxembourg
Yong Yu	Shaanxi Normal University, China
Tsz Hon Yuen	Huawei Singapore, Singapore

Additional Reviewers

Alptekin, Halit	Lin, Chengjun
Chen, Rongmao	Liu, Jianghua
Ciampi, Michele	Ma, Xinshu
Feng, Hanwen	Maitra, Subhamoy
Fernandez, Carmen	Mitakidis, Evangelos
Guo, Jingjing	Nieto, Ana
Hu, Ziyuan	Nuida, Koji
Karyda, Maria	Papamartzivanos, Dimitrios
Krzywiecki, Lukasz	Sakzad, Amin
Lauer, Hagen	Sengupta, Binanda
Leontiadis, Iraklis	Siniscalchi, Luisa
Li, Dawei	Su, Chunhua
Li, Zengpeng	Słowik, Marcin

Takashima, Katsuyuki
Takayasu, Atsushi
Tian, Haibo
Tsiatsikas, Zisis
Tzouramanis, Theodoros
Wang, Qin
Wang, Yujue
Wang, Yunling
Wang, Zheng
Watanabe, Yohei
Yang, Xu

Yu, Zuoxia
Yuan, Xingliang
Zhang, Lei
Zhang, Ning
Zhang, Wentao
Zhang, Xiao
Zhang, Xiaoyu
Zheng, Haibin
Zhu, Fei
Zhu, Youwen
Zuo, Cong

Contents

Blockchain

An Adaptive Gas Cost Mechanism for Ethereum to Defend Against Under-Priced DoS Attacks	3
<i>Ting Chen, Xiaoqi Li, Ying Wang, Jiachi Chen, Zihao Li, Xiapu Luo, Man Ho Au, and Xiaosong Zhang</i>	
A User-Friendly Centrally Banked Cryptocurrency	25
<i>Xuan Han, Yamin Liu, and Haixia Xu</i>	
Contract Coin: Toward Practical Contract Signing on Blockchain	43
<i>Haibo Tian, Jiejie He, and Liqing Fu</i>	
TTP-free Fair Exchange of Digital Signatures with Bitcoin.	62
<i>Wentao Zhang, Qianhong Wu, Bo Qin, Tianxu Han, Yanting Zhang, Xiaofeng Chen, and Na Li</i>	

Asymmetric Encryption

The KDM-CCA Security of REACT	85
<i>Jinyong Chang, Honglong Dai, and Maozhi Xu</i>	
Privacy-Preserving Extraction of HOG Features Based on Integer Vector Homomorphic Encryption	102
<i>Haomiao Yang, Yunfan Huang, Yong Yu, Mingxuan Yao, and Xiaosong Zhang</i>	
Hierarchical Conditional Proxy Re-Encryption: A New Insight of Fine-Grained Secure Data Sharing.	118
<i>Kai He, Xueqiao Liu, Huaqiang Yuan, Wenhong Wei, and Kaitai Liang</i>	
New Proof for BKP IBE Scheme and Improvement in the MIMC Setting . . .	136
<i>Song Luo, Lu Yan, Jian Weng, and Zheng Yang</i>	
A Secure Variant of the SRP Encryption Scheme with Shorter Private Key	156
<i>Bo Lv, Zhiniang Peng, and Shaohua Tang</i>	
Key Bit-Dependent Attack on Protected PKC Using a Single Trace.	168
<i>Bo-Yeon Sim and Dong-Guk Han</i>	

Group-Based Source-Destination Verifiable Encryption with Blacklist Checking	186
<i>Zhongyuan Yao, Yi Mu, and Guomin Yang</i>	

Compact Attribute-Based and Online-Offline Multi-input Inner Product Encryptions from Standard Static Assumptions (Short Paper)	204
<i>Pratish Datta</i>	

Symmetric Encryption

Optimizing Online Permutation-Based AE Schemes for Lightweight Applications	217
<i>Yu Sasaki and Kan Yasuda</i>	

Dual Relationship Between Impossible Differentials and Zero Correlation Linear Hulls of SIMON-Like Ciphers	237
<i>Xuan Shen, Ruilin Li, Bing Sun, Lei Cheng, Chao Li, and Maodong Liao</i>	

Block Cipher Modes of Operation for Heterogeneous Format Preserving Encryption	256
<i>Toshiya Shimizu and Takeshi Shimoyama</i>	

Lattice-Based Cryptography

Compact Lossy and All-but-One Trapdoor Functions from Lattice	279
<i>Leixiao Cheng, Quanshui Wu, and Yunlei Zhao</i>	

A Lattice-Based Approach to Privacy-Preserving Biometric Authentication Without Relying on Trusted Third Parties	297
<i>Trung Dinh, Ron Steinfeld, and Nandita Bhattacharjee</i>	

Enhancement for Secure Multiple Matrix Multiplications over Ring-LWE Homomorphic Encryption	320
<i>Pradeep Kumar Mishra, Dung Hoang Duong, and Masaya Yasuda</i>	

Searchable Encryption

Verifiable Range Query Processing for Cloud Computing	333
<i>Yanling Li, Junzuo Lai, Chuansheng Wang, Jianghe Zhang, and Jie Xiong</i>	

Ranked Searchable Symmetric Encryption Supporting Conjunctive Queries	350
<i>Yanjun Shen and Peng Zhang</i>	

A New Functional Encryption for Multidimensional Range Query (Short Paper)	361
<i>Jia Xu, Ee-Chien Chang, and Jianying Zhou</i>	

Signature

Linearly Homomorphic Signatures with Designated Entities	375
<i>Cheng-Jun Lin, Xinyi Huang, Shitang Li, Wei Wu, and Shao-Jun Yang</i>	
Efficient Certificate-Based Signature and Its Aggregation	391
<i>Xinxin Ma, Jun Shao, Cong Zuo, and Ru Meng</i>	
Recovering Attacks Against Linear Sketch in Fuzzy Signature Schemes of ACNS 2015 and 2016	409
<i>Masaya Yasuda, Takeshi Shimoyama, Masahiko Takenaka, Narishige Abe, Shigefumi Yamada, and Junpei Yamaguchi</i>	
Fast and Adaptively Secure Signatures in the Random Oracle Model from Indistinguishability Obfuscation (Short Paper)	422
<i>Bei Liang and Aikaterini Mitrokotsa</i>	

Authentication

EyeSec: A Practical Shoulder-Surfing Resistant Gaze-Based Authentication System	435
<i>Na Li, Qianhong Wu, Jingwen Liu, Wei Hu, Bo Qin, and Wei Wu</i>	
Enhanced Remote Password-Authenticated Key Agreement Based on Smart Card Supporting Password Changing	454
<i>Jian Shen, Meng Feng, Dengzhi Liu, Chen Wang, Jiachen Jiang, and Xingming Sun</i>	
A Practical Authentication Protocol for Anonymous Web Browsing	468
<i>Xu Yang, Xun Yi, Hui Cui, Xuechao Yang, Surya Nepal, Xinyi Huang, and Yali Zeng</i>	

Cloud Security

Dynamic Provable Data Possession Protocols with Public Verifiability and Data Privacy	485
<i>Clémentine Gritti, Rongmao Chen, Willy Susilo, and Thomas Plantard</i>	
Outsourcing Encrypted Excel Files	506
<i>Ya-Nan Li, Qianhong Wu, Wenyi Tang, Bo Qin, Qin Wang, and Meixia Miao</i>	

Outsourced Privacy-Preserving Random Decision Tree Algorithm Under Multiple Parties for Sensor-Cloud Integration	525
<i>Ye Li, Zoe L. Jiang, Xuan Wang, S. M. Yiu, and Junbin Fang</i>	
Effective Security Analysis for Combinations of MTD Techniques on Cloud Computing (Short Paper)	539
<i>Hooman Alavizadeh, Dong Seong Kim, Jin B. Hong, and Julian Jang-Jaccard</i>	
Network Security	
Fast Discretized Gaussian Sampling and Post-quantum TLS Ciphersuite	551
<i>Xinwei Gao, Lin Li, Jintai Ding, Jiqiang Liu, R. V. Saraswathy, and Zhe Liu</i>	
Automatic Encryption Schemes Based on the Neural Networks: Analysis and Discussions on the Various Adversarial Models (Short Paper)	566
<i>Yidan Zhang, Marino Anthony James, Jiageng Chen, Chunhua Su, and Jinguang Han</i>	
Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper)	576
<i>Thomas D. Wagner, Esther Palomar, Khaled Mahbub, and Ali E. Abdallah</i>	
Design and Implementation of a Lightweight Kernel-Level Network Intrusion Prevention System for Virtualized Environment (Short Paper)	587
<i>Mei-Ling Chiang, Jian-Kai Wang, Li-Chi Feng, Yang-Sen Chen, You-Chi Wang, and Wen-Yu Kao</i>	
Cyber-Physical Security	
Secure Communications in Unmanned Aerial Vehicle Network.	601
<i>Shuangyu He, Qianhong Wu, Jingwen Liu, Wei Hu, Bo Qin, and Ya-Nan Li</i>	
On the Security of In-Vehicle Hybrid Network: Status and Challenges	621
<i>Tianxiang Huang, Jianying Zhou, Yi Wang, and Anyu Cheng</i>	
IoVShield: An Efficient Vehicular Intrusion Detection System for Self-driving (Short Paper)	638
<i>Zhuo Wei, Yanjiang Yang, Yasmin Rehana, Yongdong Wu, Jian Weng, and Robert H. Deng</i>	
Enforcing Security in Artificially Intelligent Robots Using Monitors (Short Paper)	648
<i>Orhio Mark Creado and Phu Dung Le</i>	

Social Network and QR Code Security

Hello, Facebook! Here Is the Stalkers' Paradise! Design and Analysis of Enumeration Attack Using Phone Numbers on Facebook	663
<i>Jinwoo Kim, Kuyju Kim, Junsung Cho, Hyoungshick Kim, and Sebastian Schrittwieser</i>	
Covert QR Codes: How to Hide in the Crowd	678
<i>Yang-Wai Chow, Willy Susilo, and Joonsang Baek</i>	
Home Location Protection in Mobile Social Networks: A Community Based Method (Short Paper)	694
<i>Bo Liu, Wanlei Zhou, Shui Yu, Kun Wang, Yu Wang, Yong Xiang, and Jin Li</i>	

Software Security and Trusted Computing

A Formal Model for an Ideal CFI	707
<i>Sepehr Minagar, Balasubramaniam Srinivasan, and Phu Dung Le</i>	
Defending Application Cache Integrity of Android Runtime	727
<i>Jia Wan, Mohammad Zulkernine, Phil Eisen, and Clifford Liem</i>	
An Ensemble Learning System to Mitigate Malware Concept Drift Attacks (Short Paper).	747
<i>Zhi Wang, Meiqi Tian, Junnan Wang, and Chunfu Jia</i>	
Using the B Method to Formalize Access Control Mechanism with TrustZone Hardware Isolation (Short Paper)	759
<i>Lu Ren, Rui Chang, Qing Yin, and Wei Wang</i>	
Matching Function-Call Graph of Binary Codes and Its Applications (Short Paper)	770
<i>Yong Tang, Yi Wang, ShuNing Wei, Bo Yu, and Qiang Yang</i>	

SocialSec Track

Reasoning About Trust and Belief Change on a Social Network: A Formal Approach.	783
<i>Aaron Hunter</i>	
An Effective Authentication for Client Application Using ARM TrustZone	802
<i>Hang Jiang, Rui Chang, Lu Ren, Weiyu Dong, Liehui Jiang, and Shuiqiao Yang</i>	

Generic Framework for Attribute-Based Group Signature	814
<i>Veronika Kuchta, Gaurav Sharma, Rajeev Anand Sahu, and Olivier Markowitch</i>	
An Improved Leveled Fully Homomorphic Encryption Scheme over the Integers	835
<i>Xiaoqiang Sun, Peng Zhang, Jianping Yu, and Weixin Xie</i>	
The ECCA Security of Hybrid Encryptions	847
<i>Honglong Dai, Jinyong Chang, Zhenduo Hou, and Maozhi Xu</i>	
A Secure Server-Based Pseudorandom Number Generator Protocol for Mobile Devices	860
<i>Hooman Alavizadeh, Hootan Alavizadeh, Kudakwashe Dube, Dong Seong Kim, Julian Jang-Jaccard, and Hans W. Guesgen</i>	
A Secure and Practical Signature Scheme for Blockchain Based on Biometrics	877
<i>Yosuke Kaga, Masakazu Fujio, Ken Naganuma, Kenta Takahashi, Takao Murakami, Tetsushi Ohki, and Masakatsu Nishigaki</i>	
Toward Fuzz Test Based on Protocol Reverse Engineering.	892
<i>Jun Cai, Jian-Zhen Luo, Jianliang Ruan, and Yan Liu</i>	
How Spam Features Change in Twitter and the Impact to Machine Learning Based Detection	898
<i>Tingmin Wu, Derek Wang, Sheng Wen, and Yang Xiang</i>	
Author Index	905