Lecture Notes in Computer Science 10631

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

Editorial Board

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

Sihan Qing · Chris Mitchell
Liqun Chen · Dongmei Liu (Eds.)

Information and Communications Security

19th International Conference, ICICS 2017 Beijing, China, December 6–8, 2017 Proceedings

Springer

Editors
Sihan Qing
Chinese Academy of Sciences
and Peking University
Beijing
China

Chris Mitchell
Royal Holloway, University of London
Egham, Surrey
UK

Liqun Chen
University of Surrey
Guildford, Surrey
UK

Dongmei Liu
Microsoft
Beijing
China

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-89499-7 ISBN 978-3-319-89500-0 (eBook)
https://doi.org/10.1007/978-3-319-89500-0

Library of Congress Control Number: 2018939454

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG
part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 19th International Conference on Information and Communications Security (ICICS 2017) was held in Beijing, China, during December 6–8, 2017. The ICICS conference series is an established forum that brings together people from universities, research institutes, industry, and government institutions who work in a range of fields within information and communications security. The ICICS conferences give attendees the opportunity to exchange new ideas and investigate developments in the state of the art. In previous years, ICICS has taken place in Australia (1999), China (2015, 2013, 2011, 2009, 2007, 2005, 2003, 2001 and 1997), Hong Kong (2012, 2014), Singapore (2002, 2016), Spain (2010, 2004), UK (2008), and USA (2006). On each occasion, as on this one, the proceedings have been published in the Springer LNCS series.

In total, 188 manuscripts from 20 countries and districts were submitted to ICICS 2017, among which 43 regular and 14 short papers from 13 countries and districts were accepted. The accepted papers cover a wide range of disciplines within information security and applied cryptography. Each submission to ICICS 2017 was anonymously reviewed by at least three or four reviewers. We are very grateful to the Program Committee, which was composed of 72 members from 19 countries; we would like to thank them, as well as all the external reviewers, for their valuable contributions to the tough and time-consuming reviewing process. We also thank our two keynote speakers: Dr. K. P. Chow from the University of Hong Kong and Prof. Atsuko Miyaji from Osaka University of Japan.

ICICS 2017 was organized and hosted by the Institute of Information Engineering, Chinese Academy of Sciences (CAS), the Institute of Software and Microelectronics, Peking University, and the State Key Laboratory of Information Security of the Institute of Software, Chinese Academy of Sciences (CAS). ICICS 2017 was supported by the National Natural Science Foundation of China under Grant No. 61170282.

We would like to thank the authors who submitted their papers to ICICS 2017, and the attendees from all around the world. Finally, we would also like to thank Organizing Committee Chair Zhen Xu and co-chair Liming Wang for providing logistic support, Chao Zheng for managing the conference website and the EasyChair system, Publicity Chair Qingni Shen for making the wide distribution of the call for papers, and Publication Chair Dongmei Liu for her time and expertise in compiling the proceedings.

December 2017

Sihan Qing
Chris Mitchell
Liqun Chen

Organization

General Chair

Dan Meng	Institute of Information Engineering, Chinese Academy of Sciences, China

Program Chairs

Sihan Qing	Chinese Academy of Sciences and Peking University, China
Chris Mitchell	Royal Holloway, University of London, UK
Liqun Chen	University of Surrey, UK

Organizing Committee

Zhen Xu (Chair)	Institute of Information Engineering, Chinese Academy of Sciences, China
Liming Wang (Vice Chair)	Institute of Information Engineering, Chinese Academy of Sciences, China
Chao Zheng	SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China

Publicity Chair

Qingni Shen	Peking University, China

Publication Chair

Dongmei Liu	Microsoft, China

Program Committee

Man Ho Allen Au	The Hong Kong Polytechnic University, Hong Kong
Joonsang Baek	University of Wollongong, Australia
Zhenfu Cao	East China Normal University, China
Chin Chen Chang	Feng Chia University, Taiwan
Chi Chen	Institute of Information Engineering, Chinese Academy of Sciences, China
Kefei Chen	Hangzhou Normal University, China
Liqun Chen	University of Surrey, UK
Zhong Chen	Peking University, China
K. P. Chow	The University of Hong Kong, Hong Kong
Frédéric Cuppens	Telecom Bretagne, France

Naccache David	Ecole Normale Superieure, France
Josep-Lluís Ferrer-Gomila	University of the Balearic Islands, Spain
Steven Furnell	University of Plymouth, UK
Debin Gao	Singapore Management University, Singapore
Dieter Gollmann	Hamburg University of Technology, Germany
Dawu Gu	Shanghai Jiao Tong University, China
Yong Guan	Iowa State University, USA
Jinguang Han	University of Surrey, UK
Shoichi Hirose	University of Fukui, Japan
Qiong Huang	South China Agricultural University, China
Xinyi Huang	Fujian Normal University, China
Chi Kwong Hui	The University of Hong Kong, Hong Kong
Lech Janczewski	The University of Auckland, New Zealand
Chunfu Jia	Nankai University, China
Sokratis K. Katsikas	Center for Cyber and Information Security, NTNU, Norway
Howon Kim	Pusan National University, South Korea
Kwangjo Kim	Korea Advanced Institute of Science and Technology, Korea
Byoungcheon Lee	Joongbu University, South Korea
Xinghua Li	Xidian University, China
Zichen Li	Beijing Institue Graphic Communication, China
Kaitai Liang	Manchester Metropolitan University, UK
Dongdai Lin	Institute of Information Engineering, Chinese Academy of Sciences, China
Hua-Yi Lin	China University of Technology, Taiwan
Chris Mitchell	Royal Holloway, University of London, UK
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Takashi Nishide	University of Tsukuba, Japan
Takao Okubo	Institute of Information Security, Japan
Changgen Peng	Guizhou University, China
Raphael Phan	Loughborough University, Malaysia
Josef Pieprzyk	Queensland University of Technology, Australia
Jing Qin	Shandong University, China
Sihan Qing	Institute of Software, Chinese Academy of Sciences, China
Elizabeth Quaglia	Royal Holloway, University of London, UK
Kai Rannenberg	Goethe University Frankfurt, Germany
Bimal Roy	Indian Statistical Institute, Kolkata, India
Pierangela Samarati	Università degli Studi di Milano, Italy
Daniele Sgandurra	Information Security Group, Royal Holloway, UK
Qingni Shen	Peking University, China
Hung-Min Sun	National Tsing Hua University, Taiwan
Neeraj Suri	TU Darmstadt, Germany
Willy Susilo	University of Wollongong, Australia
Chunming Tang	Guangzhou University, China
Claire Vishik	Intel Corporation, UK
Guilin Wang	Huawei International Pte Ltd., Singapore

Huaxiong Wang	Nanyang Technological University, Singapore
Jingsong Wang	Tianjin University of Technology, China
Lihua Wang	National Institute of Information and Communications Technology, Japan
Liming Wang	Institute of Information Engineering, Chinese Academy of Sciences, China
Lina Wang	Wuhan University, China
Weiping Wen	Peking University, China
Jian Weng	Jinan University, China
Andreas Wespi	IBM Zurich Research Laboratory, Switzerland
Wenling Wu	Institute of Software, Chinese Academy of Sciences, China
Yingjie Wu	Fuzhou University, China
Yongdong Wu	Institute for Infocomm Research, Singapore
Zhenqiang Wu	Shaanxi Normal University, China
Shouhuai Xu	University of Texas at San Antonio, USA
Zhen Xu	Institute of Information Engineering, Chinese Academy of Sciences, China
Rui Xue	The Institute of Information Engineering, CAS, China
Min Yang	Fudan University, China
Alec Yasinsac	University of South Alabama, USA
Siu Ming Yiu	The University of Hong Kong, Hong Kong
Yong Yu	Shaanxi Normal University, China
Fangguo Zhang	Sun Yat-sen University, China
Hongli Zhang	Harbin Institute of Technology, China
Rui Zhang	Institute of Information Engineering, Chinese Academy of Sciences, China
Wentao Zhang	Institute of Information Engineering, Chinese Academy of Sciences, China
Chao Zheng	Institute of Information Engineering, Chinese Academy of Sciences, China
Yongbin Zhou	Institute of Information Engineering, Chinese Academy of Sciences, China

Additional Reviewers

Aminanto, Muhamad Erza	Chu, Cheng Kang	Jiang, Linzhi
Bao, Judong	Cui, Yuzhao	Kang, Xin
Chan, Raymond	Cuppens, Nora	Li, Baichuan
Chen, Haoyu	Fan, Limin	Li, Hongbo
Chen, Hua	Feng, Chao	Li, Huige
Chen, Zehong	Gong, Junqing	Li, Jiguo
Chen, Zhide	Guo, Qingwen	Li, Juanru
Cheng, Chen-Mou	Hamm, Peter	Li, Yannan
Choi, Rak Yong	Harborth, David	Li, Zhi
Chou, Tung	Huang, Jianye	Li, Zichen

Lin, Cheng-Jun
Liu, Jianghua
Liu, Xiangyu
Liu, Yuejun
Liu, Zhen
Liu, Zhiqiang
Long, Yu
Ma, Hui
Ma, Jinhua
Minaud, Brice
Mishra, Pradeep
Nakasho, Kazuhisa
Nan, Yuhong
Niu, Ben
Okumura, Shinya
Qin, Yu
Schmid, Michael
Schmitz, Christopher
Shen, Jiachen
Su, Chunhua
Sun, Hung-Min
Tan, Benjamin Hong Meng
Tan, Gaosheng
Tao, Yang
Tomasin, Stefano
Tsuchida, Hikaru
Wang, Fuqun
Wang, Haijiang
Wang, Huige
Wang, Licheng
Wang, Weijia
Wang, Yuntao
Wang, Zhu
Wei, Lifei
Wei, Yichen
Wen, Joy
Xiao, Yuting
Xie, Shaohao
Xu, Rui
Xu, Yanhong
Xue, Liang
Xv, Lingling
Yanai, Naoto
Yang, Rupeng
Yang, Wenbo
Yang, Yanjiang
Yuen, John
Zhang, Huang
Zhang, Juanyang
Zhang, Kai
Zhang, Lei
Zhang, Rocky
Zhang, Yuexin
Zhang, Zheng
Zhou, Shunfan

Contents

Formal Analysis and Randomness Test

Formal Analysis of a TTP-Free Blacklistable Anonymous Credentials System 3
Weijin Wang, Jingbin Liu, Yu Qin, and Dengguo Feng

An Efficiency Optimization Scheme for the On-the-Fly Statistical Randomness Test 17
Jiahui Shen, Tianyu Chen, Lei Wang, and Yuan Ma

Signature Scheme and Key Management

FABSS: Attribute-Based Sanitizable Signature for Flexible Access Structure 39
Ruo Mo, Jianfeng Ma, Ximeng Liu, and Qi Li

SSUKey: A CPU-Based Solution Protecting Private Keys on Untrusted OS 51
Huorong Li, Wuqiong Pan, Jingqiang Lin, Wangzhao Cheng, and Bingyu Li

Algorithms

The Reductions for the Approximating Covering Radius Problem 65
Wenwen Wang and Kewei Lv

Solving Discrete Logarithm Problem in an Interval Using Periodic Iterates 75
Jianing Liu and Kewei Lv

Distributed Pseudorandom Functions for General Access Structures in NP 81
Bei Liang and Aikaterini Mitrokotsa

Reducing Randomness Complexity of Mask Refreshing Algorithm 88
Shuang Qiu, Rui Zhang, Yongbin Zhou, and Hailong Zhang

Applied Cryptography

A Plausibly Deniable Encryption Scheme Utilizing PUF's Thermo-Sensitivity 105
Changting Li, Zongbin Liu, Lingchen Zhang, Cunqing Ma, and Liang Zheng

Two Efficient Tag-Based Encryption Schemes on Lattices 118
Xueqing Wang, Biao Wang, and Rui Xue

Compact (Targeted Homomorphic) Inner Product Encryption from LWE 132
Jie Li, Daode Zhang, Xianhui Lu, and Kunpeng Wang

Compact Inner Product Encryption from LWE 141
Zhedong Wang, Xiong Fan, and Mingsheng Wang

Towards Tightly Secure Deterministic Public Key Encryption. 154
Daode Zhang, Bao Li, Yamin Liu, Haiyang Xue, Xianhui Lu, and Dingding Jia

Efficient Inner Product Encryption with Simulation-Based Security 162
Qingsong Zhao, Qingkai Zeng, and Ximeng Liu

Server-Aided Directly Revocable Ciphertext-Policy Attribute-Based Encryption with Verifiable Delegation 172
Gang Yu, Xiaoxiao Ma, Zhenfu Cao, Weihua Zhu, and Guang Zeng

Practical Large Universe Attribute-Set Based Encryption in the Standard Model 180
Xinyu Feng, Cancan Jin, Cong Li, Yuejian Fang, Qingni Shen, and Zhonghai Wu

Fully Secure Hidden Ciphertext-Policy Attribute-Based Proxy Re-encryption 192
Xinyu Feng, Cong Li, Dan Li, Yuejian Fang, and Qingni Shen

Identity-Based Group Encryption Revisited 205
Kanika Gupta, S. Sharmila Deva Selvi, C. Pandu Rangan, and Shubham Sopan Dighe

Compact Hierarchical IBE from Lattices in the Standard Model 210
Daode Zhang, Fuyang Fang, Bao Li, Haiyang Xue, and Bei Liang

Attacks and Attacks Defense

Methods for Increasing the Resistance of Cryptographic Designs Against Horizontal DPA Attacks. 225
Ievgen Kabin, Zoya Dyka, Dan Kreiser, and Peter Langendoerfer

New Certificateless Public Key Encryption Secure Against Malicious KGC Attacks in the Standard Model 236
Wenjie Yang, Jian Weng, and Futai Zhang

A Lattice Attack on Homomorphic NTRU with Non-invertible Public Keys 248
Soyoung Ahn, Hyang-Sook Lee, Seongan Lim, and Ikkwon Yie

Practical Range Proof for Cryptocurrency Monero with Provable Security . . . 255
Kang Li, Rupeng Yang, Man Ho Au, and Qiuliang Xu

Wireless Sensor Network Security

Modeling Key Infection in Large-Scale Sensor Networks 265
Feiyang Peng, Zhihong Liu, Yong Zeng, and Jialei Wang

SDN-Based Secure Localization in Heterogeneous WSN 276
Meigen Huang and Bin Yu

Security Applications

A PUF and Software Collaborative Key Protection Scheme 291
Changting Li, Zongbin Liu, Lingchen Zhang, Cunqing Ma, and Liang Zheng

Towards a Trusted and Privacy Preserving Membership Service in Distributed Ledger Using Intel Software Guard Extensions 304
Xueping Liang, Sachin Shetty, Deepak Tosh, Peter Foytik, and Lingchen Zhang

Malicious Code Defense and Mobile Security

Deobfuscation of Virtualization-Obfuscated Code Through Symbolic Execution and Compilation Optimization 313
Mingyue Liang, Zhoujun Li, Qiang Zeng, and Zhejun Fang

A Self-healing Key Distribution Scheme for Mobile Ad Hoc Networks 325
Guangli Xiang, Lu Yu, Beilei Li, and Mengsen Xia

IoT Security

SecHome: A Secure Large-Scale Smart Home System Using Hierarchical Identity Based Encryption 339
Yu Li, Yazhe Wang, and Yuan Zhang

Multi-attribute Counterfeiting Tag Identification Protocol in Large-Scale RFID System 352
Dali Zhu, Wenjing Rong, Di Wu, and Na Pang

Hijacking Your Routers via Control-Hijacking URLs in Embedded Devices with Web Interfaces 363
Ming Yuan, Ye Li, and Zhoujun Li

A Method to Effectively Detect Vulnerabilities on Path Planning of VIN 374
Jingjing Liu, Wenjia Niu, Jiqiang Liu, Jia Zhao, Tong Chen, Yinqi Yang, Yingxiao Xiang, and Lei Han

Healthcare and Industrial Control System Security

Towards Decentralized Accountability and Self-sovereignty in Healthcare Systems 387
Xueping Liang, Sachin Shetty, Juan Zhao, Daniel Bowden, Danyi Li, and Jihong Liu

P3ASC: Privacy-Preserving Pseudonym and Attribute-Based Signcryption Scheme for Cloud-Based Mobile Healthcare System 399
Changji Wang, Yuan Yuan, and Shengyi Jiang

S7commTrace: A High Interactive Honeypot for Industrial Control System Based on S7 Protocol 412
Feng Xiao, Enhong Chen, and Qiang Xu

Privacy Protection

Research on Clustering-Differential Privacy for Express Data Release 427
Tianying Chen and Haiyan Kang

Frequent Itemset Mining with Differential Privacy Based on Transaction Truncation 438
Ying Xia, Yu Huang, Xu Zhang, and HaeYoung Bae

Perturbation Paradigms of Maintaining Privacy-Preserving Monotonicity for Differential Privacy 446
Hai Liu, Zhenqiang Wu, Changgen Peng, Shuangyue Zhang, Feng Tian, and Laifeng Lu

The De-anonymization Method Based on User Spatio-Temporal Mobility Trace 459
Zhenyu Chen, Yanyan Fu, Min Zhang, Zhenfeng Zhang, and Hao Li

Privacy-Preserving Disease Risk Test Based on Bloom Filters 472
Jun Zhang, Linru Zhang, Meiqi He, and Siu-Ming Yiu

Engineering Issues of Crypto

Verifiable and Forward Secure Dynamic Searchable Symmetric Encryption with Storage Efficiency 489
Kazuki Yoneyama and Shogo Kimura

Improved Automatic Search Tool for Bit-Oriented Block Ciphers and Its Applications. 502
Lingchen Li, Wenling Wu, and Lei Zhang

Hypercubes and Private Information Retrieval. 509
Anirban Basu, Rui Xu, Juan Camilo Corena, and Shinsaku Kiyomoto

A Multi-client Dynamic Searchable Symmetric Encryption System with Physical Deletion. 516
Lei Xu, Chungen Xu, Joseph K. Liu, Cong Zuo, and Peng Zhang

High-Performance Symmetric Cryptography Server with GPU Acceleration 529
Wangzhao Cheng, Fangyu Zheng, Wuqiong Pan, Jingqiang Lin, Huorong Li, and Bingyu Li

An Experimental Study of Kannan's Embedding Technique for the Search LWE Problem 541
Yuntao Wang, Yoshinori Aono, and Tsuyoshi Takagi

Cloud and E-commerce Security

A Security-Enhanced vTPM 2.0 for Cloud Computing. 557
Juan Wang, Feng Xiao, Jianwei Huang, Daochen Zha, Chengyang Fan, Wei Hu, and Huanguo Zhang

SDAC: A New Software-Defined Access Control Paradigm for Cloud-Based Systems. 570
Ruan He, Montida Pattaranantakul, Zonghua Zhang, and Thomas Duval

A Cross-Modal CCA-Based Astroturfing Detection Approach. 582
Xiaoxuan Bai, Yingxiao Xiang, Wenjia Niu, Jiqiang Liu, Tong Chen, Jingjing Liu, and Tong Wu

Security Protocols

Secure and Efficient Two-Factor Authentication Protocol Using RSA Signature for Multi-server Environments 595
Zhiqiang Xu, Debiao He, and Xinyi Huang

Authenticated Group Key Agreement Protocol Without Pairing 606
Gaurav Sharma, Rajeev Anand Sahu, Veronika Kuchta, Olivier Markowitch, and Suman Bala

Network Security

Machine Learning for Black-Box Fuzzing of Network Protocols 621
Rong Fan and Yaoyao Chang

A Novel Semantic-Aware Approach for Detecting Malicious Web Traffic . . . 633
Jing Yang, Liming Wang, and Zhen Xu

An Active and Dynamic Botnet Detection Approach to Track Hidden Concept Drift 646
Zhi Wang, Meiqi Tian, and Chunfu Jia

Statically Defend Network Consumption Against Acker Failure Vulnerability in Storm 661
Wenjun Qian, Qingni Shen, Yizhe Yang, Yahui Yang, and Zhonghai Wu

Pollution Attacks Identification in Structured P2P Overlay Networks 674
Zied Trifa, Jalel Eddine Hajlaoui, and Maher Khemakhem

Author Index 687