

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>

Guojun Wang · Indrakshi Ray
Jose M. Alcaraz Calero · Sabu M. Thampi (Eds.)

Security, Privacy, and Anonymity in Computation, Communication, and Storage

9th International Conference, SpaCCS 2016
Zhangjiajie, China, November 16–18, 2016
Proceedings

Editors

Guojun Wang
Guangzhou University
Guangzhou
China

Indrakshi Ray
Department of Computer Science
Colorado State University
Fort Collins, CO
USA

Jose M. Alcaraz Calero
University of the West of Scotland
Paisley, Glasgow
UK

Sabu M. Thampi
Indian Institute of Information Technology
and Management, Kerala (IIITMK)
Trivandrum, Kerala
India

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-49147-9

ISBN 978-3-319-49148-6 (eBook)

DOI 10.1007/978-3-319-49148-6

Library of Congress Control Number: 2016957376

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 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

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

Preface

The 9th International Conference on Security, Privacy, and Anonymity in Computation, Communication and Storage (SpaCCS 2016) was held in Zhangjiajie, China, during November 16–18, 2016, and was jointly organized by Central South University, Guangzhou University, and Jishou University.

The SpaCCS conference series provides a forum for world-class researchers to gather and share their research achievements, emerging ideas, and trends in information security fields. Previous SpaCCS conferences were held in Helsinki, Finland (2015), Beijing, China (2014), Melbourne, Australia (2013), Liverpool, UK (2012), and Changsha, China (2011).

This year the conference received 110 submissions. All submissions received at least three reviews during a high-quality review process. According to the review results, 40 papers were selected for oral presentation at the conference and inclusion in this Springer volume, giving an acceptance rate of 36.4 %. Besides the regular paper presentations, the program included three interesting and insightful keynotes by Prof. Yang Xiao, the University of Alabama, USA, Prof. Indrakshi Ray, Colorado State University, USA, and Dr. Shui Yu, Deakin University, Australia. We are very grateful to the keynote speakers.

SpaCCS 2016 was made possible by the joint effort of numerous people and organizations worldwide. There is a long list of people who volunteered their time and energy to put together the conference and who deserve special thanks. First and foremost, we would like to offer our gratitude to Prof. Guojun Wang from Guangzhou University, China, and Prof. Gregorio Martinez from University of Murcia, Spain, the Steering Committee chairs, for guiding the whole process of the conference. We are also deeply grateful to all the Program Committee members for their great effort in reading, commenting, debating, and finally selecting the papers. We also wish to thank all the external reviewers for assisting the Program Committee in their particular areas of expertise.

We would like to offer our gratitude to the general chairs, Jianbin Li, Prof. Felix Gomez Marmol, and Prof. Juan E. Tapiador, for their great support and good suggestions contributing to the success of the conference. Thanks also go to the: workshop chairs, Dr. Raymond Choo, Dr. Mianxiong Dong, and Dr. Jin Li; publicity chairs, Prof. Carlos Becker Westphall, Dr. Scott Fowler, and Dr. Xiaofei Xing; publication chair, Shuhong Chen; organization chairs, Prof. Fang Qi, Dr. Xiaofei Xing and Prof. Qingping Zhou; registration chair, Ms. Pin Liu; conference secretariat, Dr. Sancheng Peng; and Webmaster, Mr. Binji Mo.

We would like to thank all the authors, participants, and session chairs for their valuable efforts, many of whom travelled long distances to attend this conference and make their valuable contributions.

November 2016

Indrakshi Ray
Jose M. Alcaraz Calero
Sabu M. Thampi

Organization

General Chairs

Jianbin Li	Central South University, China
Felix Gomez Marmol	NEC Laboratories Europe, Germany
Juan E. Tapiador	The University Carlos III of Madrid, Spain

Program Chairs

Indrakshi Ray	Colorado State University, USA
Jose M. Alcaraz Calero	University of the West of Scotland, UK
Sabu M. Thampai	Indian Institute of Information Technology and Management, India

Program Vice Chairs

Security Track

Javier Lopez	University of Malaga, Spain
Qin Liu	Hunan University, China

Privacy Track

Rinku Dewri	University of Denver, USA
Wenjun Jiang	Hunan University, China

Anonymity Track

Mario Freire	The University of Beira Interior, Portugal
Md. Zakirul Alam Bhuiyan	Temple University, USA

Program Committee

Afrand Agah	West Chester University of Pennsylvania, USA
Habtamu Abie	Norwegian Computing Center/Norsk Regnesentral, Norway
Hamid Ali Abed Al-asadi	Basra University, Iraq
Ricardo Marco Alaez	University of the West of Scotland, UK
Bruhadeshwar Bezawada	International Institute of Information Technology, India
Cataldo Basile	Politecnico di Torino, Italy
Simona Bernardi	Centro Universitario de la Defensa, Spain
Jorge Bernal Bernabe	University of Murcia, Spain
Saad Bani-Mohammad	Dean of IT College, Al al-Bayt University, Jordan

Salima Benbernou	Université Paris Descartes, France
Yan Bai	University of Washington Tacoma, USA
Miguel Pupo Correia	University of Lisbon, Portugal
Alfredo Cuzzocrea	University of Trieste and ICAR-CNR, Italy, Italy
Aniello Castiglione	University of Salerno, Italy
Anupam Chattopadhyay	Nanyang Technological University, Singapore
Christian Callegari	The University of Pisa, Italy
John A. Clark	University of York, UK
Lien-Wu Chen	Feng Chia University, Taiwan
Mauro Conti	University of Padua, Italy
Naveen Chilamkurti	La Trobe University, Australia
Sudip Chakraborty	Valdosta State University, USA
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalonia
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Ying Dai	Temple University, USA
Yucong Duan	Hainan University, China
Zhihui Du	Tsinghua University, China
Oscar Esparza	Universitat Politècnica de Catalunya, Spain
Dieter Gollmann	Hamburg University of Technology, Germany
Dimitris Geneiatakis	Aristotle University of Thessaloniki, Greece
Liang Gu	Yale University, USA
Saurabh Kumar Garg	University of Tasmania, Australia
Yao Guo	Peking University, China
Ying Guo	Central South University, China
Ching-Hsien Hsu	Chung Hua University, Taiwan
Mohammad Mehedi Hassans	King Saud University, KSA
Ragib Hasan	University of Alabama, Birmingham, UK
Xiaojun Hei	School of Electronic Information and Communications, Huazhong University of Science and Technology, China
Xinyi Huang	Fujian Normal University, China
Pedro Inácio	University of Beira Interior, Portugal
Hai Jiang	Arkansas State University, USA
Murtuza Jadhwal	Wichita State University, USA
Young-Sik Jeong	Dongguk University, Korea
Gabor Kiss	Obuda University, Hungary
Ram Krishnan	University of Texas, USA
Ryan Ko	University of Waikato, New Zealand
Vana Kalogeraki	Athens University of Economics, Greece
Chi Lin	Dalian University of Technology, China
Giovanni Livraga	Università degli Studi di Milano, Italy
Haibing Lu	Santa Clara University, USA
Haitao Lang	University of Physics & Electronics, China
Jialin Liu	Lawrence Berkeley National Lab, USA

Rongxing Lu	Nanyang Technological University, Singapore
Xin Li	Nanjing University of Aeronautics and Astronautics, China
Xin Liao	Hunan University, China
Yingjiu Li	Singapore Management University, Singapore
Guerroumi Mohamed	University of Sciences and Technology Houari Boumediene, Algeria
Jose Andre Morales	Carnegie Mellon University-CERT, USA
Aleksandra Mileva	University Goce Delcev, Republic of Macedonia
Juan Pedro Munoz-Gea	Universidad Politécnica de Cartagena, Spain
Mirco Marchetti	University of Modena and Reggio Emilia, Italy
Renita Murimi	Oklahoma Baptist University, USA
Sheikh M. Habib	TU Darmstadt Germany, Germany
Subhomoy Maitra	ISI Calcutta, India
Wissam Mallouli	Montimage, France
Ben Niu	Lehigh University, USA
David Naccache	École normale supérieure, France
Pouya Ostovari	Temple University, USA
Rolf Oppliger	eSECURITY Technologies, Switzerland
Al-Sakib Khan Pathan	UAP and SEU, Bangladesh/Islamic University in Madinah, KSA
Carlos Perez-Conde	Universidad de Valencia, Spain
Günther Pernul	University of Regensburg, Germany
Joon S. Park	Syracuse University, USA
Risat Mahmud Pathan	Chalmers University of Technology, Sweden
Roberto Di Pietro	Nokia Bell Labs, France
Sancheng Peng	Guangdong University of Foreign Studies, China
Miguel Pardal	University of Lisbon, Portugal
Vincenzo Piuri	Università degli Studi di Milano, Italy
Zeeshan Pervez	University of the West of Scotland, UK
Bimal Roy	Indian Statistical Institute, India
Imed Romdhani	Edinburgh Napier University, UK
Indrajit Ray	Colorado State University, USA
Md. Abdur Razzaque	University of Dhaka, Bangladesh
Mubashir Husain Rehmani	COMSATS Institue of Information Technology, Pakistan
Altair Santin	Pontifical Catholic University of Parana, Brazil
Chang-ai Sun	University of Science and Technology Beijing, China
Chao Song	University of Electronic Science and Technology of China, China
Chunhua Su	School of Information Science, Japan
Dimitris E. Simos	SBA Research, Austria
Hossain Shahriar	Kennesaw State University, USA
Hung-Min Sun	National Tsing Hua University, Taiwan
Jun Shen	University of Wollongong, Australia

Junggab Son	North Carolina Central University, USA
Qiang Tang	University of Luxembourg, Luxembourg
Ramakrishna Thurimella	University of Denver, USA
Traian Marius Truta	Northern Kentucky University, USA
Eugene Y. Vasserman	Kansas State University, USA
Luis Javier Garcia Villalba	The Complutense University, Spain
Tam Vu	University of Colorado-De, USA
Hejun Wu	Sun Yat-Sen University, China
Mingzhong Wang	University of the Sunshine Coast, Australia
Yongdong Wu	Insitute for Infocomm Research, Singapore
Yunsheng Wang	Kettering University, USA
Xiaolong Xu	Nanjing University of Posts and Telecommunications, China
Baoliu Ye	Nanjing University, China
Chau Yuen	Singapore University of Technology and Design, Singapore
Yu Hua	Huazhong University of Science and Technology, China
Ilusun You	Soonchunhyang University, Republic of Korea
Lin Ye	Harbin Institute of Technology, China
Muneer Masadeh Bani Yassein	Jordan University of Science and Technology, Jordan
Shucheng Yu	University of Arkansas at Little Rock, USA
Xuanxia Yao	Universty of Science and Technology Beijing, China
Congxu Zhu	Central South University, China
David Zheng	Frostburg State University, USA
Huan Zhou	China Three Gorges University, China
Mingwu Zhang	Hubei University of Technology, China
Qingchen Zhang	St. Francis Xavier University, Canada
Sherali Zeadally	University of Kentucky, USA
Yaoxiong Zhao	Google Inc, USA
Youwen Zhu	Nanjing University of Aeronautics and Astronautics, China
Yun-Wei Zhao	Tilburg University, The Netherlands

Steering Committee Chairs

Guojun Wang	Guangzhou University, China
Gregorio Martinez	University of Murcia, Spain

Steering Committee

Jemal H. Abawajy	Deakin University, Australia
Jose M. Alcaraz Calero	University of the West of Scotland, UK
Giannong Cao	Hong Kong Polytechnic University, Hong Kong, SAR China

Hsiao-Hwa Chen	National Cheng Kung University, Taiwan
Jinjun Chen	University of Technology, Sydney, Australia
Kim-Kwang Raymond Choo	University of Texas at San Antonio, USA
Robert Deng	Singapore Management University, Singapore
Mario Freire	The University of Beira Interior, Portugal
Minyi Guo	Shanghai Jiao Tong University, China
Weijia Jia	Shanghai Jiao Tong University, China
Wei Jie	University of West London, UK
Georgios Kambourakis	University of the Aegean, Greece
Ryan Ko	University of Waikato, New Zealand
Constantinos Kolias	George Mason University, USA
Jianbin Li	Central South University, China
Jie Li	University of Tsukuba, Japan
Jianhua Ma	Hosei University, Japan
Felix Gomez Marmol	NEC Laboratories Europe, Germany
Geyong Min	University of Exeter, UK
Peter Mueller	IBM Zurich Research Laboratory, Switzerland
Indrakshi Ray	Colorado State University, USA
Kouichi Sakurai	Kyushu University, Japan
Juan E. Tapiador	The University Carlos III of Madrid, Spain
Sabu M. Thampi	Indian Institute of Information Technology and Management, India
Jie Wu	Temple University, USA
Yang Xiao	The University of Alabama, USA
Yang Xiang	Deakin University, Australia
Zheng Yan	Aalto University, Finland
Laurence T. Yang	St. Francis Xavier University, Canada
Wanlei Zhou	Deakin University, Australia

Workshop Chairs

Kim-Kwang Raymond Choo	University of Texas at San Antonio, USA
Mianxiong Dong	Muroran Institute of Technology, Japan
Jin Li	Guangzhou University, China

Publicity Chairs

Carlos Becker Westphall	Federal University of Santa Catarina, Brazil
Scott Fowler	Linköping University, Sweden
Xiaofei Xing	Guangzhou University, China

Publication Chair

Shuhong Chen	Hunan Institute of Engineering, China
--------------	---------------------------------------

Registration Chair

Pin Liu Central South University, China

Local Chairs

Fang Qi Central South University, China
Xiaofei Xing Guangzhou University, China
Qingping Zhou Jishou University, China

Conference Secretariat

Sancheng Peng Guangdong University of Foreign Studies, China

Webmaster

Binji Mo Central South University, China

SpaCCS 2016 Sponsors



Contents

A Lightweight RFID Authentication Protocol with Forward Security and Randomized Identifier	1
<i>Zhicai Shi, Fei Wu, Changzhi Wang, and Shitao Ren</i>	
A Security Proxy Scheme Based on Attribute Node Mapping for Cloud Storage	14
<i>Huakang Li, Zhenyu Wang, Yitao Yang, and Guozi Sun</i>	
Privacy Preserving Scheme for Location and Content Protection in Location-Based Services.	26
<i>Tao Peng, Qin Liu, Guojun Wang, and Yang Xiang</i>	
An Improved Asymmetric Searchable Encryption Scheme	39
<i>Qi Wu</i>	
Recommendation Systems in Real Applications: Algorithm and Parallel Architecture	45
<i>Mengxian Li, Wenjun Jiang, and Kenli Li</i>	
Big Data Security Analytic for Smart Grid with Fog Nodes	59
<i>Wenlin Han and Yang Xiao</i>	
A Reduction Method of Analyzing Data-Liveness and Data-Boundedness for a Class of E-commerce Business Process Nets.	70
<i>Wangyang Yu, Guanjun Liu, and Leifeng He</i>	
Computation of Secure Consistency for Real Systems	84
<i>Mimi Wang, Guanjun Liu, Changjun Jiang, and Chungang Yan</i>	
Study on Personalized Location Privacy Protection Algorithms for Continuous Queries in LBS	98
<i>Jiayi Gan, Hongyun Xu, Mengzhen Xu, Kai Tian, Yaohui Zheng, and Yong Zhang</i>	
A Novel Signature Generation Approach in Noisy Environments for Detecting Polymorphic Worm	109
<i>Jie Wang and Jie Wu</i>	
A User Authentication Scheme Based on Trusted Platform for Cloud Computing.	122
<i>Jiaqing Mo, Zhongwang Hu, and Yuhua Lin</i>	

ROP-Hunt: Detecting Return-Oriented Programming Attacks in Applications	131
<i>Lu Si, Jie Yu, Lei Luo, Jun Ma, Qingbo Wu, and Shasha Li</i>	
On the Security of a Threshold Anonymous Authentication Protocol for VANETs	145
<i>Jianhong Zhang, Zhibin Sun, Shuai Liu, and Pengyan Liu</i>	
The Encryption Scheme with Data Compression Based on QC-LDPC	156
<i>Yiliang Han</i>	
Location Privacy Preserving Scheme Based on Attribute Encryption	164
<i>Xi Lin, Yiliang Han, Yan Ke, and Xiaoyuan Yang</i>	
Attribute-Based Traceable Anonymous Proxy Signature Strategy for Mobile Healthcare.	178
<i>Dacheng Meng, Wenbo Wang, Entao Luo, and Guojun Wang</i>	
A Privacy Preserving Friend Discovery Strategy Using Proxy Re-encryption in Mobile Social Networks	190
<i>Entao Luo, Wenbo Wang, Dacheng Meng, and Guojun Wang</i>	
Defect Analysis and Risk Assessment of Mainstream File Access Control Policies	204
<i>Li Luo, Hongjun He, and Jiao Zhu</i>	
A Comprehensive Survey of Privacy-Preserving in Smart Grid	213
<i>Guanlin Si, Zhitao Guan, Jing Li, Peng Liu, and Hong Yao</i>	
Ghost Train for Anonymous Communication	224
<i>Przemysław Błażkiewicz, Mirosław Kutyłowski, Jakub Lemiesz, and Małgorzata Sulkowska</i>	
Efficient Detection Method for Data Integrity Attacks in Smart Grid	240
<i>Peixiu An and Zhitao Guan</i>	
Fully Secure Unbounded Revocable Key-Policy Attribute-Based Encryption Scheme	251
<i>Changji Wang, Jian Fang, and Jianguo Xie</i>	
A Privacy-Preserving Hybrid Cooperative Searching Scheme over Outsourced Cloud Data	265
<i>Qiang Zhang, Qin Liu, and Guojun Wang</i>	
Modeling and Propagation Analysis on Social Influence Using Social Big Data	279
<i>Sancheng Peng, Shengyi Jiang, and Pengfei Yin</i>	

FASRP: A Fully Anonymous Security Routing Protocol in MANETs	292
<i>Jun Pan, Lin Ma, and Kai Yu</i>	
Privacy Protection in Mobile Recommender Systems: A Survey	305
<i>Kun Xu and Zheng Yan</i>	
Security in Software-Defined-Networking: A Survey	319
<i>Zhen Yao and Zheng Yan</i>	
Building Root of Trust for Report with Virtual AIK and Virtual PCR Usage for Cloud	333
<i>Qiang Huang, Dehua Zhang, Le Chang, and Jinhua Zhao</i>	
On the Impact of Location Errors on Localization Attacks in Location- Based Social Network Services	343
<i>Hanni Cheng, Shiling Mao, Minhui Xue, and Xiaojun Hei</i>	
Service-Oriented Workflow Executability from a Security Perspective	358
<i>Sardar Hussain, Richard O. Sinnott, and Ron Poet</i>	
Distributed Multi-authority Attribute-Based Encryption for Secure Friend Discovery and Data Sharing in Mobile Social Networks	374
<i>Fang Qi, Wenbo Wang, and Zhe Tang</i>	
Modeling Attack Process of Advanced Persistent Threat	383
<i>Weina Niu, Xiaosong Zhan, Kenli Li, Guowu Yang, and Ruidong Chen</i>	
A New Image Encryption Scheme Using a Hyperchaotic System	392
<i>Chong Fu, Ming Tie, Jian-lin Wang, Shao-ting Chen, and Hui-yan Jiang</i>	
Architectural Patterns for Security-Oriented Workflows in Collaborative Environments	406
<i>Sardar Hussain, Richard O. Sinnott, and Ron Poet</i>	
Modeling and Vulnerable Points Analysis for E-commerce Transaction System with a Known Attack	422
<i>Mimi Wang, Guanjun Liu, Chungang Yan, and Changjun Jiang</i>	
Authentication and Transaction Verification Using QR Codes with a Mobile Device	437
<i>Yang-Wai Chow, Willy Susilo, Guomin Yang, Man Ho Au, and Cong Wang</i>	
Secure and Efficient Mobile Payment Using QR Code in an Environment with Dishonest Authority	452
<i>Xiaoling Zhu, Zhengfeng Hou, Donghui Hu, and Jing Zhang</i>	

User Preference-Based Spamming Detection with Coupled Behavioral Analysis.	466
<i>Frank Jiang, Mingdong Tang, and Quang Anh Tran</i>	
Analysis of SIFT Method Based on Swarm Intelligent Algorithms for Copy-Move Forgery Detection.	478
<i>Fei Zhao, Wenchang Shi, Bo Qin, and Bin Liang</i>	
Encryption Scheme Based on Hyperelliptic Curve Cryptography.	491
<i>Asha Liza John and Sabu M. Thampi</i>	
Author Index	507