

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/7409>

Giovanni Livraga · Sencun Zhu (Eds.)

Data and Applications Security and Privacy XXXI

31st Annual IFIP WG 11.3 Conference, DBSec 2017
Philadelphia, PA, USA, July 19–21, 2017
Proceedings

Editors

Giovanni Livraga 
Università degli Studi di Milano
Crema
Italy

Sencun Zhu
Pennsylvania State University
Philadelphia, PA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-61175-4 ISBN 978-3-319-61176-1 (eBook)
DOI 10.1007/978-3-319-61176-1

Library of Congress Control Number: 2017943855

LNCS Sublibrary: SL3 – Information Systems and Applications, incl. Internet/Web, and HCI

© IFIP International Federation for Information Processing 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 selected for presentation at the 31st Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2017), held in Philadelphia, PA, USA, on July 19–21, 2017.

In response to the call for papers of this edition, 59 submissions were received, and all submissions were evaluated on the basis of their significance, novelty, and technical quality. The Program Committee, comprising 45 members, performed an excellent task and with the help of additional reviewers all submissions went through a careful anonymous review process (three or more reviews per submission). The Program Committee's work was carried out electronically, yielding intensive discussions. Of the submitted papers, 21 full papers and nine short papers were selected for presentation at the conference.

The success of DBSec 2017 depends on the volunteering effort of many individuals, and there is a long list of people who deserve special thanks. We would like to thank all the members of the Program Committee and all the external reviewers, for all their hard work in evaluating the papers and for their active participation in the discussion and selection process. We are very grateful to all people who gave their assistance and ensured a smooth organization process, in particular Krishna Kant and Peng Liu for their efforts as DBSec 2017 General Chairs; Sabrina De Capitani di Vimercati (IFIP WG11.3 Chair) for her guidance and support; and Fengjun Li (Publicity Chair) for helping with publicity. A special thanks goes to the keynote speaker, who accepted our invitation to deliver a keynote talk at the conference.

Last but certainly not least, thanks to all the authors who submitted papers and all the conference attendees. We hope you find the proceedings of DBSec 2017 interesting, stimulating, and inspiring for your future research.

July 2017

Giovanni Livraga
Sencun Zhu

Yingjiu Li	Singapore Management University, Singapore
Javier Lopez	University of Málaga, Spain
Fabio Martinelli	IIT-CNR, Italy
Catherine Meadows	NRL, USA
Aziz Mohaisen	SUNY Buffalo, USA
Martin Olivier	University of Pretoria, South Africa
Stefano Paraboschi	Università degli Studi di Bergamo, Italy
Günther Pernul	Universität Regensburg, Germany
Silvio Ranise	FBK Security and Trust Unit, Italy
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Pierangela Samarati	Università degli Studi di Milano, Italy
Ravi Sandhu	University of Texas at San Antonio, USA
Andreas Schaad	WIBU-SYSTEMS AG, Germany
Scott Stoller	Stony Brook University, USA
Tamir Tassa	The Open University of Israel, Israel
Mahesh Tripunitara	University of Waterloo, Canada
Jaideep Vaidya	Rutgers University, USA
Cong Wang	City University of Hong Kong, Hong Kong, SAR China
Lingyu Wang	Concordia University, Canada
Edgar Weippl	Vienna University of Technology, Austria
Yi Yang	Fontbonne University, USA
Meng Yu	University of Texas at San Antonio, USA
ShengZhi Zhang	Florida Institute of Technology, USA
Yuqing Zhang	Chinese Academy of Sciences, China
Quanyan Zhu	New York University, USA

Additional Reviewers

Isaac Agudo	Rudolf Mayer
Hafiz Asif	Alessio Merlo
Anis Bkakria	Georg Merzdovnik
Daniel Borbor	Meisam Mohamady
Juntao Chen	David Nuñez
Luis Del Vasto	Javier Parra
Philip Derbeko	Alexander Puchta
Sebastian Groll	Stefan Rass
Panagiotis Kintis	Johannes Säger
Michael Kunz	Ankit Shah
Giovanni Lagorio	Jordi Soria-Comas
Costas Lambrinouidakis	Tanay Talukdar
Suryadipta Majumdar	Iman Vakilinia
Sergio Martínez	Andrea Valenza

Sridhar Venkatesan
Akrivi Vlachou
Wei Wang
Xingjie Yu

Wanyu Zang
Mengyuan Zhang
Rui Zhang
Tao Zhang

Contents

Access Control

Cryptographically Enforced Role-Based Access Control for NoSQL Distributed Databases	3
<i>Yossif Shalabi and Ehud Gudes</i>	
Resilient Reference Monitor for Distributed Access Control via Moving Target Defense	20
<i>Dieudonne Mulamba and Indrajit Ray</i>	
Preventing Unauthorized Data Flows	41
<i>Emre Uzun, Gennaro Parlato, Vijayalakshmi Atluri, Anna Lisa Ferrara, Jaideep Vaidya, Shamik Sural, and David Lorenzi</i>	
Object-Tagged RBAC Model for the Hadoop Ecosystem	63
<i>Maanak Gupta, Farhan Patwa, and Ravi Sandhu</i>	
Identification of Access Control Policy Sentences from Natural Language Policy Documents.	82
<i>Masoud Narouei, Hamed Khanpour, and Hassan Takabi</i>	
Fast Distributed Evaluation of Stateful Attribute-Based Access Control Policies	101
<i>Thang Bui, Scott D. Stoller, and Shikhar Sharma</i>	

Privacy

Gaussian Mixture Models for Classification and Hypothesis Tests Under Differential Privacy	123
<i>Xiaosu Tong, Bowei Xi, Murat Kantarcioglu, and Ali Inan</i>	
Differentially Private K-Skyband Query Answering Through Adaptive Spatial Decomposition	142
<i>Ling Chen, Ting Yu, and Rada Chirkova</i>	
Mutually Private Location Proximity Detection with Access Control	164
<i>Michael G. Solomon, Vaidy Sunderam, Li Xiong, and Ming Li</i>	
Privacy-Preserving Elastic Net for Data Encrypted by Different Keys - With an Application on Biomarker Discovery.	185
<i>Jun Zhang, Meiqi He, and Siu-Ming Yiu</i>	

Privacy-Preserving Community-Aware Trending Topic Detection in Online Social Media 205
Theodore Georgiou, Amr El Abbadi, and Xifeng Yan

Privacy-Preserving Outlier Detection for Data Streams. 225
Jonas Böhrer, Daniel Bernau, and Florian Kerschbaum

Undoing of Privacy Policies on Facebook 239
Vishwas T. Patil and R.K. Shyamasundar

Cloud Security

Towards Actionable Mission Impact Assessment in the Context of Cloud Computing 259
Xiaoyan Sun, Anoop Singhal, and Peng Liu

Reducing Security Risks of Clouds Through Virtual Machine Placement 275
Jin Han, Wanyu Zang, Songqing Chen, and Meng Yu

Firewall Policies Provisioning Through SDN in the Cloud 293
Nora Cuppens, Salaheddine Zerkane, Yanhuang Li, David Espes, Philippe Le Parc, and Frédéric Cuppens

Budget-Constrained Result Integrity Verification of Outsourced Data Mining Computations. 311
Bo Zhang, Boxiang Dong, and Wendy Wang

Searchable Encryption to Reduce Encryption Degradation in Adjustably Encrypted Databases 325
Florian Kerschbaum and Martin Härterich

Efficient Protocols for Private Database Queries 337
Tushar Kanti Saha, Mayank, and Takeshi Koshiba

Toward Group-Based User-Attribute Policies in Azure-Like Access Control Systems 349
Anna Lisa Ferrara, Anna Squicciarini, Cong Liao, and Truc L. Nguyen

Secure Storage in the Cloud

High-Speed High-Security Public Key Encryption with Keyword Search 365
Rouzbeh Behnia, Attila Altay Yavuz, and Muslum Ozgur Ozmen

HardIDX: Practical and Secure Index with SGX 386
Benny Fuhry, Raad Bahmani, Ferdinand Brasser, Florian Hahn, Florian Kerschbaum, and Ahmad-Reza Sadeghi

A Novel Cryptographic Framework for Cloud File Systems and CryFS,
 a Provably-Secure Construction 409
*Sebastian Messmer, Jochen Rill, Dirk Achenbach,
 and Jörn Müller-Quade*

Secure Systems

Keylogger Detection Using a Decoy Keyboard 433
Seth Simms, Margot Maxwell, Sara Johnson, and Julian Rrushi

The Fallout of Key Compromise in a Proxy-Mediated Key
 Agreement Protocol 453
David Nuñez, Isaac Agudo, and Javier Lopez

Improving Resilience of Biometric Based Continuous Authentication
 with Multiple Accelerometers 473
Tim Van hamme, Davy Preuveneers, and Wouter Joosen

Security in Networks and Web

A Content-Aware Trust Index for Online Review Spam Detection 489
Hao Xue and Fengjun Li

Securing Networks Against Unpatchable and Unknown Vulnerabilities
 Using Heterogeneous Hardening Options 509
Daniel Borbor, Lingyu Wang, Sushil Jajodia, and Anoop Singhal

A Distributed Mechanism to Protect Against DDoS Attacks 529
Negar Mosharraf, Anura P. Jayasumana, and Indrakshi Ray

Securing Web Applications with Predicate Access Control 541
Zhaomo Yang and Kirill Levchenko

Author Index 555