

*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, Zürich, 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>

Silvio Ranise · Vipin Swarup (Eds.)

# Data and Applications Security and Privacy XXX

30th Annual IFIP WG 11.3 Conference, DBSec 2016  
Trento, Italy, July 18–20, 2016  
Proceedings

*Editors*

Silvio Ranise  
Fondazione Bruno Kessler  
Trento  
Italy

Vipin Swarup  
The Mitre Corp  
McLean, VA  
USA

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-41482-9              ISBN 978-3-319-41483-6 (eBook)  
DOI 10.1007/978-3-319-41483-6

Library of Congress Control Number: 2016942496

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

© IFIP International Federation for Information Processing 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 Switzerland

# Preface

These proceedings contain the papers selected for presentation at the 30th IFIP WG 11.3 Conference on Data and Applications Security (DBSec16), held in Trento, Italy, July 18–20, 2016.

DBSec16 received 54 submissions that were evaluated on the basis of their significance, novelty, technical quality, and appropriateness to the DBSec audience. Each paper was reviewed by at least three members of the Program Committee. After intensive reviewing and electronic discussions, 17 full papers and 7 short papers were selected for presentation at the conference. Their topics cover a wide range of data and application security and privacy problems including those of mobile devices, collaborative systems, databases, big data, virtual systems, cloud computing, and social networks. The program also included two invited talks.

We would like to thank all the people who invested their time and energy to make this year's edition of DBSec happen. In particular, we thank the authors for submitting their manuscripts and the attendees for contributing to the conference discussion. We are also very grateful to the members of the Program Committee and to the external reviewers for carefully reviewing and discussing the submissions, and for their commitment to meeting the strict deadlines.

We thank the people at Springer for their assistance in publishing these proceedings. Last but certainly not least, our thanks go to everybody involved in the organization of the event, most notably to Sabrina De Capitani di Vimercati (IFIP WG 11.3 Chair) for her guidance and support, Alessandro Armando (Conference Chair), Giovanni Livraga (Publicity Chair), Roberto Carbone (Local Organization Chair), and Federico Sinigaglia (Web Master).

We hope you find the proceedings of DBSec16 interesting, stimulating, and inspiring for your future research.

July 2016

Silvio Ranise  
Vipin Swarup

# Organization

## Program Committee

### Program Chairs

Silvio Ranise  
Vipin Swarup

Fondazione Bruno Kessler, Trento, Italy  
The MITRE Corporation, USA

### Members

Vijay Atluri  
Joachim Biskup  
Achim D. Brucker  
Soon Ae Chun  
Frédéric Cuppens  
Nora Cuppens-Boulahia  
Jun Dai  
Sabrina De Capitani di Vimercati  
Josep Domingo-Ferrer  
Carmen Fernández-Gago  
Simon Foley  
Sara Foresti  
Joaquin Garcia-Alfaro  
Ehud Gudes  
Yuan Hong  
Florian Kerschbaum  
Ram Krishnan  
Adam J. Lee  
Yingjiu Li  
Peng Liu  
Javier Lopez  
Sjouke Mauw  
Charles Morisset  
Martin Olivier  
Stefano Paraboschi  
Günther Pernl  
Indrakshi Ray  
Kui Ren  
Pierangela Samarati  
Ravi Sandhu  
Scott Stoller  
Tamir Tassa

Rutgers University, USA  
Technische Universität Dortmund, Germany  
The University of Sheffield, UK  
CUNY, USA  
Telecom Bretagne, France  
Telecom Bretagne, France  
California State University, Sacramento, USA  
Università degli Studi di Milano, Italy  
Universitat Rovira i Virgili, Spain  
University of Malaga, Spain  
University College Cork, Ireland  
Università degli Studi di Milano, Italy  
Telecom SudParis, France  
Ben-Gurion University, Israel  
University at Albany, SUNY, USA  
SAP, Germany  
University of Texas at San Antonio, USA  
University of Pittsburgh, USA  
Singapore Management University, Singapore  
The Pennsylvania State University, USA  
University of Malaga, Spain  
University of Luxembourg, Luxembourg  
Newcastle University, UK  
University of Pretoria, South Africa  
Università di Bergamo, Italy  
Universität Regensburg, Germany  
Colorado State University, USA  
State University of New York at Buffalo, USA  
Università degli Studi di Milano, Italy  
University of Texas at San Antonio, USA  
Stony Brook University, USA  
The Open University of Israel, Israel

Mahesh Tripunitara	University of Waterloo, Canada
Jaideep Vaidya	Rutgers University, USA
Lingyu Wang	Concordia University, Canada
Meng Yu	University of Texas at San Antonio, USA
Nicola Zannone	Eindhoven University of Technology, The Netherlands
Shengzhi Zhang	Florida Tech, USA

### **Additional Reviewers**

Ahmed, Tahmina	Mulamba, Dieudonne
Al Lail, Mustafa	Nieto, Ana
Blanco-Justicia, Alberto	Nuñez, David
Carmichael, Peter	Pieczul, Olgierd
Casas-Roma, Jordi	Ren, Chuangang
Chang, Bing	Ribes-González, Jordi
Chen, Bo	Ricci, Sara
Cheng, Yao	Rizzo, Nicholas
Fuchs, Ludwig	Romero-Tris, Cristina
Ghosh, Sudipto	Sprissler, Ethan
Hachana, Safaa	Sun, Xiaoyan
Hassan, Sabri	Sural, Shamik
Herzberg, Michael	Trujillo, Rolando
Hummer, Matthias	Xie, Xing
Idrees, Sabir	Yoon, Eunjung
Imran-Daud, Malik	Yu, Xingjie
Iovino, Vincenzo	Zang, Wanyu
Kywe, Su Mon	Zhang, Yang
Moataz, Tarik	Zhao, Mingyi

### **IFIP WG 11.3 Chair**

Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
----------------------------------	---

# Contents

## Mobile Security and Privacy

Deciphering Text from Touchscreen Key Taps . . . . .	3
<i>Haritabh Gupta, Shamik Sural, Vijayalakshmi Atluri, and Jaideep Vaidya</i>	
The Fréchet/Manhattan Distance and the Trajectory Anonymisation Problem. . . . .	19
<i>Christof Ferreira Torres and Rolando Trujillo-Rasua</i>	

## Security and Privacy in Databases

Guaranteeing Correctness of Bulk Operations in Outsourced Databases . . . . .	37
<i>Luca Ferretti, Michele Colajanni, and Mirco Marchetti</i>	
Enhanced Functionality and Confidentiality for Database Search and Publish/Subscribe Protocols . . . . .	52
<i>Giovanni Di Crescenzo, Euthimios Panagos, and Brian Coan</i>	
Privacy Preserving Probabilistic Record Linkage Using Locality Sensitive Hashes . . . . .	61
<i>Ibrahim Lazrig, Toan Ong, Indrajit Ray, Indrakshi Ray, and Michael Kahn</i>	

## Access Control

Mining Hierarchical Temporal Roles with Multiple Metrics . . . . .	79
<i>Scott D. Stoller and Thang Bui</i>	
Inter-ReBAC: Inter-operation of Relationship-Based Access Control Model Instances . . . . .	96
<i>Jason Crampton and James Sellwood</i>	
Role-Centric Circle-of-Trust in Multi-tenant Cloud IaaS. . . . .	106
<i>Navid Pustchi and Ravi Sandhu</i>	
A Comparison of Logical-Formula and Enumerated Authorization Policy ABAC Models . . . . .	122
<i>Prosunjit Biswas, Ravi Sandhu, and Ram Krishnan</i>	
Access Control for the Shuffle Index . . . . .	130
<i>Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Gerardo Pelosi, and Pierangela Samarati</i>	



**Protection and Privacy of Data and Big Data**

Private and Secure Secret Shared MapReduce (Extended Abstract) . . . . . 151  
*Shlomi Dolev, Yin Li, and Shantanu Sharma*

Towards Creating Believable Decoy Project Folders for Detecting  
 Data Theft . . . . . 161  
*Stefan Thaler, Jerry den Hartog, and Milan Petkovic*

Practical Differentially Private Modeling of Human Movement Data . . . . . 170  
*Harichandan Roy, Murat Kantarcioglu, and Latanya Sweeney*

A Practical Framework for Executing Complex Queries over Encrypted  
 Multimedia Data . . . . . 179  
*Fahad Shaon and Murat Kantarcioglu*

**Security and Privacy in Social Networks and Collaborative Systems**

Data Governance and Transparency for Collaborative Systems . . . . . 199  
*Rauf Mahmudlu, Jerry den Hartog, and Nicola Zannone*

Sharing-Habits Based Privacy Control in Social Networks . . . . . 217  
*Silvie Levy, Ehud Gudes, and Nurit Gal-Oz*

Counteracting Active Attacks in Social Network Graphs . . . . . 233  
*Sjouke Mauw, Rolando Trujillo-Rasua, and Bochuan Xuan*

**Reasoning about Security and Its Cost**

Formalizing Threat Models for Virtualized Systems. . . . . 251  
*Daniele Sgandurra, Erisa Karafili, and Emil Lupu*

Reasoning About Firewall Policies Through Refinement and Composition . . . 268  
*Ultan Neville and Simon N. Foley*

CheapSMC: A Framework to Minimize Secure Multiparty Computation  
 Cost in the Cloud . . . . . 285  
*Erman Pattuk, Murat Kantarcioglu, Huseyin Ulusoy, and Bradley Malin*

Diversifying Network Services Under Cost Constraints for Better  
 Resilience Against Unknown Attacks . . . . . 295  
*Daniel Borbor, Lingyu Wang, Sushil Jajodia, and Anoop Singhal*

Reasoning About Privacy Properties of Architectures Supporting Group  
 Authentication and Application to Biometric Systems . . . . . 313  
*Julien Bringer, Hervé Chabanne, Daniel Le Métayer, and Roch Lescuyer*

**Trust and Zero-Day Vulnerabilities**

Whom You Gonna Trust? A Longitudinal Study on TLS Notary Services . . . 331  
*Georg Merzdovnik, Klaus Falb, Martin Schmiedecker,  
 Artemios G. Voyiatzis, and Edgar Weippl*

Runtime Detection of Zero-Day Vulnerability Exploits in Contemporary  
 Software Systems . . . . . 347  
*Olgierd Pieczul and Simon N. Foley*

**Author Index** . . . . . 365