

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Lingyu Wang Basit Shafiq (Eds.)

Data and Applications Security and Privacy XXVII

27th Annual IFIP WG 11.3 Conference, DBSec 2013
Newark, NJ, USA, July 15-17, 2013
Proceedings



Springer

Volume Editors

Lingyu Wang
Concordia University
Concordia Institute for Information Systems Engineering (CIISE)
1455 de Maisonneuve Blvd. West, Montreal, QC H3G 1M8, Canada
E-mail: wang@ciise.concordia.ca

Basit Shafiq
Lahore University of Management Sciences (LUMS)
Department of Computer Science
DHA, Lahore Cantt., Lahore 54792, Pakistan
E-mail: basit@lums.edu.pk

ISSN 0302-9743
ISBN 978-3-642-39255-9
DOI 10.1007/978-3-642-39256-6
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-39256-6

Library of Congress Control Number: 2013941388

CR Subject Classification (1998): C.2.0, K.6.5, C.2, D.4.6, E.3, H.4, C.3, H.2.7-8, E.1

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

© IFIP International Federation for Information Processing 2013

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at the 27th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2013). The conference, hosted at Rutgers University, Newark, NJ, USA, during July 15–17, 2013, offered outstanding research contributions to the field of data and applications security and privacy. This year’s conference, for the first time at DBSec, presented both the Best Paper Award and the Best Student Paper Award.

In response to the call for papers, 45 papers were submitted to the conference. Each paper was reviewed by at least three, and on average 4.04, members of the Program Committee, on the basis of its significance, novelty and technical quality. The review process was followed by intensive discussions over a period of one week. Of the papers submitted, 16 full papers and six short papers were accepted for presentation at the conference. The conference program also includes two invited talks by Johannes Gehrke (Cornell University) and Vincent Poor (Princeton University). The accepted papers cover diverse research themes, ranging from classic topics, such as access control and privacy, to emerging issues, such as security and privacy in data outsourcing, mobile computing, and cloud computing.

The success of this conference was the result of the efforts of many people. We would especially like to thank Claudio Agostino Ardagna (Publicity Chair), Reza Curtmola and Heechang Shin (Local Arrangements Chairs), and Vijayalakshmi Atluri (IFIP WG 11.3 Chair). We would also thank the Program Committee members and the external reviewers for their hard work in reviewing and discussing the papers. We gratefully acknowledge all authors who submitted papers for enhancing the standards of this conference. Last but not least, thanks to all the attendees. We hope you will enjoy reading the proceedings.

July 2013

Jaideep Vaidya
Soon Ae Chun
Lingyu Wang
Basit Shafiq

Organization

Executive Committee

General Chair

Jaideep Vaidya Rutgers University, USA

General Co-chair

Soon Ae Chun Rutgers University, USA

Program Chair

Lingyu Wang Concordia University, Canada

Program Co-chair

Basit Shafiq Lahore University of Management Sciences,
Pakistan

Publicity Chair

Claudio Agostino Ardagna University of Milan, Italy

Local Arrangements Chairs

Reza Curtmola New Jersey Institute of Technology, USA
Heechang Shin Iona College, USA

IFIP WG 11.3 Chair

Vijayalakshmi Atluri Rutgers University, USA

Program Committee

Gail-Joon Ahn Arizona State University, USA
Claudio Agostino Ardagna Università degli Studi di Milano, Italy
Vijay Atluri Rutgers University, USA
Joachim Biskup Technische Universität Dortmund, Germany
Marina Blanton University of Notre Dame, USA

VIII Organization

David Chadwick	University of Kent, UK
Soon Ae Chun	Columbia University and City University of New York, USA
Frédéric Cuppens	TELECOM Bretagne, France
Nora Cuppens-Boulahia	Telecom Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Mourad Debbabi	Concordia University, Canada
Josep Domingo-Ferrer	Rovira i Virgili University, Spain
Eduardo B. Fernandez	Florida Atlantic University, USA
Simone Fischer-Huebner	Karlstad University, Sweden
Sara Foresti	Università degli Studi di Milano, Italy
Ehud Gudes	Ben-Gurion University, Israel
Ragib Hasan	University of Alabama at Birmingham, USA
Sushil Jajodia	George Mason University, USA
Sokratis Katsikas	University of Piraeus, Greece
Adam J. Lee	University of Pittsburgh, USA
Yingjiu Li	Singapore Management University, Singapore
Javier Lopez	University of Malaga, Spain
Emil Lupu	Imperial College London, UK
Martin Olivier	University of Pretoria, South Africa
Stefano Paraboschi	Università di Bergamo, Italy
Wolter Pieters	Delft University of Technology, The Netherlands
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Kui Ren	State University of New York at Buffalo, USA
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Basit Shafiq	Lahore University of Management Sciences, Pakistan
Heechang Shin	Iona College, USA
Anoop Singhal	National Institute of Standards and Technology, USA
Traian Marius Truta	Northern Kentucky University, USA
Jaideep Vaidya	Rutgers University, USA
Lingyu Wang	Concordia University, Canada
Meng Yu	Virginia Commonwealth University, USA
Xinwen Zhang	Huawei Research Center, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Zutao Zhu	Google Inc., USA

Additional Reviewers

Wanyu Zang	Zhan Qin	Amril Syalim
Wei Huo	Chao Zhang	Alessandra De
Tobias Pulls	Yosr Jarraya	Benedictis
Yifei Wang	Rodrigo Roman	Nurit Gal-Oz
Wen Ming Liu	Cornelia Tadros	Michael
Chunhua Su	Meixing Le	Emirkanian-Bouchard
Jordi Soria-Comas	Tarik Moataz	Massimiliano Albanese
Sara Hajian	Liang Cai	Tantan Liu
Dima Alhadidi	Yihua Zhang	Rolando Trujillo-Rasua
Mikhail Strizhov	Shams Zawoad	Ruben Rios
Rose-Mharie Ahlfeldt	Yoshikazu Hanatani	Rasib H. Khan
Md Munirul Haque	Daisuke Moriyama	Safaa Hachana
Bagus Santoso	Stere Preda	Ramadan Abdunabi
William Garrison	Junpei Kawamoto	Ruoyu Wu
Qingji Zheng	Zhan Wang	

Table of Contents

Privacy I

Extending Loose Associations to Multiple Fragments	1
<i>Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Giovanni Livraga, Stefano Paraboschi, and Pierangela Samarati</i>	
Database Fragmentation with Encryption: Under Which Semantic Constraints and A Priori Knowledge Can Two Keep a Secret?	17
<i>Joachim Biskup and Marcel Preuß</i>	
Differentially Private Multi-dimensional Time Series Release for Traffic Monitoring	33
<i>Liyue Fan, Li Xiong, and Vaidy Sunderam</i>	

Access Control

Policy Analysis for Administrative Role Based Access Control without Separate Administration	49
<i>Ping Yang, Mikhail Gofman, and Zijiang Yang</i>	
Toward Mining of Temporal Roles	65
<i>Barsha Mitra, Shamik Sural, Vijayalakshmi Atluri, and Jaideep Vaidya</i>	
Towards User-Oriented RBAC Model	81
<i>Haibing Lu, Yuan Hong, Yanjiang Yang, Lian Duan, and Nazia Badar</i>	

Cloud Computing

Hypervisor Event Logs as a Source of Consistent Virtual Machine Evidence for Forensic Cloud Investigations	97
<i>Sean Thorpe, Indrajit Ray, Tyrone Grandison, Abbie Barbir, and Robert France</i>	
<i>TerraCheck</i> : Verification of Dedicated Cloud Storage	113
<i>Zhan Wang, Kun Sun, Sushil Jajodia, and Jiwu Jing</i>	

Privacy II

Fair Private Set Intersection with a Semi-trusted Arbiter	128
<i>Changyu Dong, Liqun Chen, Jan Camenisch, and Giovanni Russello</i>	

Bloom Filter Bootstrap: Privacy-Preserving Estimation of the Size of an Intersection 145
Hiroaki Kikuchi and Jun Sakuma

Using Safety Constraint for Transactional Dataset Anonymization 164
Bechara Al Bouna, Chris Clifton, and Qutaibah Malluhi

Data Outsourcing

Practical Immutable Signature Bouquets (PISB) for Authentication and Integrity in Outsourced Databases 179
Attila A. Yavuz

Optimal Re-encryption Strategy for Joins in Encrypted Databases 195
Florian Kerschbaum, Martin Härterich, Patrick Grofig, Mathias Kohler, Andreas Schaad, Axel Schröpfer, and Walter Tighzert

Access Control and Query Verification for Untrusted Databases 211
Rohit Jain and Sunil Prabhakar

Mobile Computing

Quantitative Security Risk Assessment of Android Permissions and Applications 226
Yang Wang, Jun Zheng, Chen Sun, and Srinivas Mukkamala

A Model for Trust-Based Access Control and Delegation in Mobile Clouds 242
Indrajit Ray, Dieudonne Mulamba, Indrakshi Ray, and Keesook J. Han

Short Papers

Result Integrity Verification of Outsourced Frequent Itemset Mining 258
Boxiang Dong, Ruilin Liu, and Hui (Wendy) Wang

An Approach to Select Cost-Effective Risk Countermeasures 266
Le Minh Sang Tran, Bjørnar Solhaug, and Ketil Stølen

Enhance Biometric Database Privacy: Defining Privacy-Preserving Drawer Size Standard for the Setbase 274
Benjamin Justus, Frédéric Cuppens, Nora Cuppens-Boulahia, Julien Bringer, Hervé Chabanne, and Olivier Capiere

Rule Enforcement with Third Parties in Secure Cooperative Data Access 282
Meixiang Le, Krishna Kant, and Sushil Jajodia

Unlinkable Content Playbacks in a Multiparty DRM System	289
<i>Ronald Petrlc and Stephan Sekula</i>	
Analysis of TRBAC with Dynamic Temporal Role Hierarchies	297
<i>Emre Uzun, Vijayalakshmi Atluri, Jaideep Vaidya, and Shamik Sural</i>	
Author Index	305