

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

Willem Jonker Milan Petković(Eds.)

Secure Data Management

8th VLDB Workshop, SDM 2011
Seattle, WA, USA, September 2, 2011
Proceedings

Volume Editors

Willem Jonker
University of Twente
Faculty of Electrical Engineering,
Mathematics and Computer Science
P.O. Box 217, 7500 AE Enschede
The Netherlands
E-mail: willem.jonker@ictlabs.eu

Milan Petković
Philips Research Europe
High Tech Campus 34
5656 AE Eindhoven
The Netherlands
E-mail: milan.petkovic@philips.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-23555-9 e-ISSN 978-3-642-23556-6
DOI 10.1007/978-3-642-23556-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011934809

CR Subject Classification (1998): K.6.5, D.4.6, E.3, C.2, H.4, H.3

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

© Springer-Verlag Berlin Heidelberg 2011

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

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 year was the eighth edition of the VLDB Secure Data Management Workshop. The topic of data security remains an important area of research especially due to the steady growing proliferation of emerging data services such as cloud computing, location-based services, and health-related services. Confidentiality is the main driver for the research that covers topics such as privacy-enhancing technologies, access control, and search in encrypted data.

We received 19 submissions of which the Program Committee selected 10 papers to be presented at the workshop and included in the proceedings (approx. 50% acceptance rate). We hope the papers collected in this volume will stimulate your research in this area.

The regular papers in the proceedings are grouped into three sections. The first section focuses on privacy. The papers in this section present a study in privacy violations followed by application-driven work on algorithms. The second section focuses on data security in networks. The papers address issues related to management of confidential data that are stored in cloud and sensor networks. The third section groups a collection of more basic secure data management techniques that can find their way toward many different application settings.

We wish to thank all the authors of submitted papers for their high-quality submissions. We would also like to thank the Program Committee members as well as additional referees for doing an excellent review job. Finally, let us acknowledge Luan Ibraimi who helped in the technical preparation of the proceedings.

September 2011

Willem Jonker
Milan Petković

Organization

Workshop Organizers

Willem Jonker	EIT ICT Labs /University of Twente, The Netherlands
Milan Petković	Philips Research/Eindhoven University of Technology, The Netherlands

Program Committee

Imad Abbadi	Oxford University, UK
Gerrit Bleumer	Francotyp-Postalia, Germany
Ljiljana Brankovic	University of Newcastle, Australia
Sabrina De Capitani di Vimercati	University of Milan, Italy
Ernesto Damiani	University of Milan, Italy
Deng Mina	Philips Research, The Netherlands
Eric Diehl	Techicolor, France
Jeroen Doumen	Irdeto, The Netherlands
Csilla Farkas	University of South Carolina, USA
Eduardo Fernandez-Medina Paton	Universidad de Castilla-La Mancha, Spain
Elena Ferrari	Università degli Studi dell'Insubria, Italy
Simone Fischer-Hübner	Karlstad University, Sweden
Tyrone Grandison	IBM Research, USA
Dieter Gollmann	Technische Universität Hamburg-Harburg, Germany
Marit Hansen	Independent Centre for Privacy Protection, Germany
Min-Shiang Hwang	National Chung Hsing University, Taiwan
Mizuho Iwaihara	Waseda University, Japan
Sushil Jajodia	George Mason University, USA
Ton Kalker	Huawei, USA
Marc Langheinrich	University of Lugano (USI), Switzerland
Nguyen Manh Tho	Vienna University of Technology, Austria
Sharad Mehrotra	University of California at Irvine, USA
Stig Frode Mjølsnes	Norwegian University of Science and Technology, Norway
Eiji Okamoto	University of Tsukuba, Japan
Sylvia Osborn	University of Western Ontario, Canada

VIII Organization

Günther Pernul	University of Regensburg, Germany
Birgit Pfitzmann	IBM Watson Research Lab, Switzerland
Bart Preneel	KU Leuven, Belgium
Kai Rannenberg	Goethe University Frankfurt, Germany
Ahmad-Reza Sadeghi	Darmstadt University, Germany
Andreas Schaad	SAP Labs, France
Jason Smith	Queensland University of Technology, Australia
Morton Swimmer	Forward-looking Threat Research, Trend Micro, Germany
Clark Thomborson	University of Auckland, New Zealand
Sheng Zhong	State University of New York at Buffalo, USA

Additional Referee

Carlos Blanco	Universidad de Castilla-La Mancha, Spain
---------------	--

Table of Contents

Privacy Protection and Quantification

Quantifying Privacy Violations	1
<i>Mishtu Banerjee, Rosa Karimi Adl, Leanne Wu, and Ken Barker</i>	
On-the-Fly Generalization Hierarchies for Numerical Attributes Revisited	18
<i>Alina Campan, Nicholas Cooper, and Traian Marius Truta</i>	
LORA: Link Obfuscation by Randomization in Graphs	33
<i>Qian Xiao, Zhengkui Wang, and Kian-Lee Tan</i>	

Security in Cloud and Sensor Networks

A Comprehensive Framework for Secure Query Processing on Relational Data in the Cloud	52
<i>Shiyuan Wang, Divyakant Agrawal, and Amr El Abbadi</i>	
Challenges in Secure Sensor-Cloud Computing	70
<i>Nayot Poolsappasit, Vimal Kumar, Sanjay Madria, and Sriram Chellappan</i>	
SensorSafe: A Framework for Privacy-Preserving Management of Personal Sensory Information	85
<i>Haksoo Choi, Supriyo Chakraborty, Zainul M. Charbiwala, and Mani B. Srivastava</i>	

Secure Data Management Technologies

Watermarking for Adaptive Streaming Protocols	101
<i>Dmitri Jarnikov and Jeroen M. Doumen</i>	
Conjunctive Wildcard Search over Encrypted Data	114
<i>Christoph Bösch, Richard Brinkman, Pieter Hartel, and Willem Jonker</i>	
Adjusting the Trade-Off between Privacy Guarantees and Computational Cost in Secure Hardware PIR	128
<i>Spiridon Bakiras and Konstantinos F. Nikolopoulos</i>	
Purpose Control: Did You Process the Data for the Intended Purpose?	145
<i>Milan Petković, Davide Prandi, and Nicola Zannone</i>	

Author Index	169
--------------------	-----