

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

University of Dortmund, 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 of Computer Science, Saarbruecken, Germany

Willem Jonker Milan Petković (Eds.)

Secure Data Management

6th VLDB Workshop, SDM 2009
Lyon, France, August 28, 2009
Proceedings

Volume Editors

Willem Jonker

Philips Research Europe

High Tech Campus 34, 5656 AE Eindhoven, The Netherlands

and University of Twente, Department of Computer Science

P.O. Box 217, 7500 AE Enschede, The Netherlands

E-mail: willem.jonker@philips.com

Milan Petković

Koninklijke Philips Electronics N.V., Philips Research Laboratories

High Tech Campus 34, 5656 AE Eindhoven, The Netherlands

E-mail: Milan.Petkovic@philips.com

Library of Congress Control Number: 2009933478

CR Subject Classification (1998): E.3, H.2.7, K.4.4, K.6.5, C.2

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

ISSN 0302-9743

ISBN-10 3-642-04218-X Springer Berlin Heidelberg New York

ISBN-13 978-3-642-04218-8 Springer Berlin Heidelberg New York

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

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

Printed on acid-free paper SPIN: 12752188 06/3180 5 4 3 2 1 0

Preface

The new emerging technologies put new requirements on security and data management. As data are accessible anytime anywhere, it becomes much easier to get unauthorized data access. Furthermore, the use of new technologies has brought some privacy concerns. It becomes simpler to collect, store, and search personal information thereby endangering people's privacy. Therefore, research in secure data management is gaining importance, attracting the attention of both the data management and the security research communities. The interesting problems range from traditional topics, such as, access control and general database security, via privacy protection to new research directions, such as cryptographically enforced access control and encrypted databases.

This year, the call for papers attracted 24 papers both from universities and industry. For presentation at the workshop, the Program Committee selected 10 full papers (41% acceptance rate). These papers are collected in this volume, which we hope will serve as a useful research and reference material.

The papers in the proceeding are grouped into three sections. The first section focuses on database security which remains an important research area. The papers in this section address several interesting topics including query optimization in encrypted databases, database provenance, database intrusion detection, and confidence policy compliant query evaluation. The second section changes the focal point to the topic of access control. The papers in this section deal with provenance access control, access control model for collaborative editors, self-modifying access control policies, and enforcing access control on XML documents. The third section focuses on privacy protection addressing the privacy issues around location-based services and anonymity/diversity for the micro-data release problem.

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.

July 2009

Willem Jonker
Milan Petković

Organization

Workshop Organizers

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

Program Committee

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
Eric Diehl	Thomson Research, France
Lee Dong Hoon	Korea University, Korea
Jeroen Doumen	Irdeto, The Netherlands
Csilla Farkas	University of South Carolina, USA
Eduardo Fernández-Medina	University of Castilla-La Mancha, Spain
Elena Ferrari	University of Insubria, Italy
Simone Fischer-Hübner	Karlstad University, Sweden
Tyrone Grandison	IBM Almaden Research Center, 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	Kyoto University, Japan
Sushil Jajodia	George Mason University, USA
Ton Kalker	HP Labs, USA
Marc Langheinrich	Università della Svizzera italiana (USI), Switzerland
Nguyen Manh Tho	Vienna University of Technology, Austria
Nick Mankovich	Philips Medical Systems, USA
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
Günther Pernul	University of Regensburg, Germany
Birgit Pfitzmann	IBM Watson Research Lab, Switzerland

VIII Organization

Bart Preneel
Kai Rannenberg
Andreas Schaad
Nicholas Sheppard
Jason Smith
Morton Swimmer

Clark Thomborson
Sheng Zhong

KU Leuven, Belgium
Goethe University Frankfurt, Germany
SAP Labs, France
University of Calgary, Canada
Queensland University of Technology, Australia
John Jay College of Criminal Justice/CUNY,
USA
University of Auckland, New Zealand
State University of New York at Buffalo, USA

Additional Referees

Hans Hedbom
Luan Ibraimi
Leonardo Martucci
Mike Radmacher
Falk Wagner
Lei Zhang

Karlstad University, Sweden
Twente University, The Netherlands
Karlstad University, Sweden
Goethe University Frankfurt, Germany
Goethe University Frankfurt, Germany
George Mason University, USA

Table of Contents

Database Security

Query Optimization in Encrypted Relational Databases by Vertical Schema Partitioning	1
<i>Mustafa Canim, Murat Kantarcioglu, and Ali Inan</i>	
Do You Know Where Your Data's Been? – Tamper-Evident Database Provenance.....	17
<i>Jing Zhang, Adriane Chapman, and Kristen LeFevre</i>	
Database Intrusion Detection Using Role Profiling with Role Hierarchy	33
<i>Garfield Zhiping Wu, Sylvia L. Osborn, and Xin Jin</i>	
Query Processing Techniques for Compliance with Data Confidence Policies	49
<i>Chenyun Dai, Dan Lin, Murat Kantarcioglu, Elisa Bertino, Ebru Celikel, and Bhavani Thuraisingham</i>	

Access Control

An Access Control Language for a General Provenance Model	68
<i>Qun Ni, Shouhuai Xu, Elisa Bertino, Ravi Sandhu, and Weili Han</i>	
A Flexible Access Control Model for Distributed Collaborative Editors	89
<i>Abdessamad Imine, Asma Cherif, and Michaël Rusinowitch</i>	
On the Construction and Verification of Self-modifying Access Control Policies	107
<i>David Power, Mark Slaymaker, and Andrew Simpson</i>	
Controlling Access to XML Documents over XML Native and Relational Databases	122
<i>Lazaros Koromilas, George Chinis, Irini Fundulaki, and Sotiris Ioannidis</i>	

Privacy Protection

Longitude: Centralized Privacy-Preserving Computation of Users' Proximity	142
<i>Sergio Mascetti, Claudio Bettini, and Dario Freni</i>	
L-Cover: Preserving Diversity by Anonymity	158
<i>Lei Zhang, Lingyu Wang, Sushil Jajodia, and Alexander Brodsky</i>	
Author Index	173