

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

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

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Willem Jonker Milan Petković (Eds.)

Secure Data Management

VLDB 2004 Workshop, SDM 2004
Toronto, Canada, August 30, 2004
Proceedings

Volume Editors

Willem Jonker

Milan Petković

Information and System Security, Philips Research Eindhoven

Prof. Holstlaan 4, 5656 AA Eindhoven, Netherlands

E-mail: {willem.jonker, milan.petkovic}@philips.com

Library of Congress Control Number: 2004110614

CR Subject Classification (1998): H.2.0, H.2, C.2.0, H.3, E.3, D.4.6, K.6.5

ISSN 0302-9743

ISBN 3-540-22983-3 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 is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik

Printed on acid-free paper SPIN: 11312253 06/3142 5 4 3 2 1 0

Preface

Concepts like ubiquitous computing and ambient intelligence that exploit increasingly interconnected networks and mobility put new requirements on data management. An important element in the connected world is that data will be accessible anytime anywhere. This also has its downside in that it becomes easier to get unauthorized data access. Furthermore, it will become easier to collect, store, and search personal information and endanger people's privacy. As a result security and privacy of data becomes more and more of an issue. Therefore, secure data management, which is also privacy-enhanced, turns out to be a challenging goal that will also seriously influence the acceptance of ubiquitous computing and ambient intelligence concepts by society.

With the above in mind, we organized the SDM 2004 workshop to initiate and promote secure data management as one of the important interdisciplinary research fields that brings together people from the security research community and the data management research community. The call for papers attracted 28 submissions both from universities and industry. The program committee selected 15 research papers for presentation at the workshop. The technical contributions presented at the SDM workshop are collected in this volume, which, we hope, will serve as a valuable research and reference book in your professional life.

The volume is divided into four topical parts. The first section focuses on accessing encrypted data. The first three papers of this section concentrate on the interesting problem of searching in encrypted data, while the last paper discusses the integrity of data that is shared or exchanged on the World-Wide Web. The second section addresses private data management, as well as management of private (personal) data. Research topics of this section include management of personal data with P3P for Internet services, privacy in digital rights management, as well as privacy-preserving data mining. The third section focuses on access control, which remains an important area of interest for database security researchers. Finally, two papers in the fourth section discuss specific topics within database security: release control of sensitive associations stored in databases, and a method to defend against copying a database as a whole.

Workshop Organizers

Willem Jonker (Philips Research/University of Twente, The Netherlands)

Milan Petković (Philips Research, The Netherlands)

Program Committee

Rakesh Agrawal, IBM Almaden Research Center, USA

Peter Apers, Twente University, The Netherlands

Elisa Bertino, CERIAS, Purdue University, USA

Ljiljana Branković, University of Newcastle, Australia

Sabrina De Capitani di Vimercati, University of Milan, Italy

Ernesto Damiani, University of Milan, Italy

Eric Diehl, Thomson Research, France

Csilla Farkas, University of South Carolina, USA

Eduardo Fernández-Medina, University of Castilla-La Mancha, Spain

Marit Hansen, Independent Centre for Privacy Protection, Germany

Pieter Hartel, Twente University, The Netherlands

Ton Kalker, HP Research, USA

Marc Langheinrich, Institute for Pervasive Computing, ETH Zurich, Switzerland

Sylvia Osborn, University of Western Ontario, Canada

Bart Preneel, KU Leuven, Belgium

Jean-Jacques Quisquater, Université Catholique de Louvain, Belgium

Morton Swimmer, IBM Zurich Research Lab, Switzerland

Bhavani Thuraisingham, National Science Foundation, USA

Additional Referees

Sandro Etalle, University of Twente, The Netherlands

Ling Feng, University of Twente, The Netherlands

Table of Contents

Encrypted Data Access

Secure and Privacy Preserving Outsourcing of Tree Structured Data	1
<i>Ping Lin and K. Selçuk Candan</i>	
Using Secret Sharing for Searching in Encrypted Data	18
<i>Richard Brinkman, Jeroen Doumen, and Willem Jonker</i>	
A Structure Preserving Database Encryption Scheme	28
<i>Yuval Elovici, Ronen Waisenberg, Erez Shmueli, and Ehud Gudes</i>	
Modeling Integrity in Data Exchange	41
<i>Gerome Miklau and Dan Suciu</i>	

Privacy Preserving Data Management

Experimental Analysis of Privacy-Preserving Statistics Computation	55
<i>Hiranmayee Subramaniam, Rebecca N. Wright, and Zhiqiang Yang</i>	
Achieving Privacy Preservation when Sharing Data for Clustering	67
<i>Stanley R.M. Oliveira and Osmar R. Zaïane</i>	
Privacy-Preserving Digital Rights Management	83
<i>Claudine Conrado, Milan Petković, and Willem Jonker</i>	
Management of Private Data: Addressing User Privacy and Economic, Social, and Ethical Concerns	100
<i>Dawn Jutla, Peter Bodorik, and Deyun Gao</i>	

Access Control

PeerTrust: Automated Trust Negotiation for Peers on the Semantic Web . .	118
<i>Wolfgang Nejdl, Daniel Olmedilla, and Marianne Winslett</i>	
A Flexible Framework for Architecting XML Access Control Enforcement Mechanisms	133
<i>Bo Luo, Dongwon Lee, Wang-Chien Lee, and Peng Liu</i>	
Abstracting and Refining Authorization in SQL	148
<i>Arnon Rosenthal and Edward Sciore</i>	
A Classifier-Based Approach to User-Role Assignment for Web Applications	163
<i>Shengli Sheng and Sylvia L. Osborn</i>	

LTAM: A Location-Temporal Authorization Model 172
Hai Yu and Ee-Peng Lim

Database Security

Identifying Sensitive Associations in Databases for Release Control 187
Claudio Bettini, Xiaoyang Sean Wang, and Sushil Jajodia

Using Delay to Defend Against Database Extraction 202
Magesh Jayapandian, Brian Noble, James Mickens, and H.V. Jagadish

Author Index 219