Lecture Notes in Computer Science 4165

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Willem Jonker Milan Petković (Eds.)

Secure Data Management

Third VLDB Workshop, SDM 2006
Seoul, Korea, September 10-11, 2006
Proceedings

Volume Editors

Willem Jonker
Philips Research Europe
High Tech Campus 34
5656 AE Eindhoven
The Netherlands
E-mail: willem.jonker@philips.com

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

Library of Congress Control Number: 2006931629

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

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

ISSN 0302-9743
ISBN-10 3-540-38984-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-38984-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11844662 06/3142 5 4 3 2 1 0

Preface

Recent developments in computer, communication, and information technologies, along with increasingly interconnected networks and mobility have established new emerging technologies, such as ubiquitous computing and ambient intelligence, as a very important and unavoidable part of everyday life. However, this development has greatly influenced people's security concerns. As data is accessible anytime from anywhere, according to these new concepts, it becomes much easier to get unauthorized data access. As another consequence, the use of new technologies has brought some privacy concerns. It becomes simpler to collect, store, and search personal information and endanger people's privacy. Therefore, research in the area of secure data management is of growing importance, attracting the attention of both the data management and security research communities. The interesting problems range from traditional ones such as access control (with all variations, like role-based and/or context-aware), database security, operations on encrypted data, and privacy preserving data mining to cryptographic protocols.

The call for papers attracted 33 papers both from universities and industry. The program committee selected 13 research papers for presentation at the workshop. These papers are also collected in this volume, which we hope will serve you as useful research and reference material.

The volume is divided roughly into four major sections. The first section focuses on privacy protection addressing the topics of indistinguishability, sovereign information sharing, data anonymization, and privacy protection in ubiquitous environments. The second section changes slightly the focal point to privacy preserving data management. The papers in this section deal with search on encrypted data and privacy preserving clustering. The third section focuses on access control which remains an important area of interest. The papers cover role-based access control, XML access control and conflict resolution. The last section addresses database security topics.

Finally, let us acknowledge the work of Richard Brinkman, who helped in the technical preparation of these proceedings.

July 2006 Willem Jonker and Milan Petković

Organization

Workshop Organizers

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

Program Committee

Gerrit Bleumer, Francotyp-Postalia, Germany
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
Ling Feng, Twente University, Netherlands
Eduardo Fernández-Medina, University of Castilla-La Mancha, Spain
Elena Ferrari, Università degli Studi dell'Insubria, Italy
Simone Fischer-Hübner, Karlstad University, Sweden
Tyrone Grandison, IBM Almaden Research Center, USA
Ehud Gudes, Ben-Gurion University, Israel
Hacan Hacigümüş, IBM Almaden Research Center, USA
Marit Hansen, Independent Centre for Privacy Protection, Germany
Pieter Hartel, Twente University, The Netherlands
Dong Hoon Lee, Korea University, Korea
Mizuho Iwaihara, Kyoto University, Japan
Sushil Jajodia George Mason University, USA
Ton Kalker, HP Research, USA
Marc Langheinrich, Institute for Pervasive Computing ETH Zurich, Switzerland
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 Zurich Research Lab, Switzerland
Bart Preneel, KU Leuven, Belgium
Kai Rannenberg, Goethe University Frankfurt, Germany
Andreas Schaad, SAP Labs, France
Morton Swimmer, IBM Zurich Research Lab, Switzerland
Sheng Zhong, Stevens Institute of Technology, USA

Additional Referees

Srikanth Akkiraju, University of Twente, The Netherlands
Richard Brinkman, University of Twente, The Netherlands
Ileana Buhan, University of Twente, The Netherlands
Lothar Fritsch, Johann Wolfgang Goethe University, Germany
Ludwig Fuchs, University of Regensburg, Germany
Bijit Hore, University of California at Irvine, USA
Ravi Chandra Jammalamadaka, University of California at Irvine, USA
Heiko Rossnagel, Johann Wolfgang Goethe University, Germany
Falk Wagner, Johann Wolfgang Goethe University, Germany
Lingyu Wang, George Mason University, USA
Chao Yao, George Mason University, USA
Xingbo Yu, University of California at Irvine, USA

Table of Contents

Privacy Protection

Indistinguishability: The Other Aspect of Privacy 1
Chao Yao, Lingyu Wang, Sean X. Wang, Sushil Jajodia

Sovereign Information Sharing Among Malicious Partners 18
Stefan Böttcher, Sebastian Obermeier

Temporal Context Lie Detection and Generation 30
Xiangdong An, Dawn Jutla, Nick Cercone

Secure Anonymization for Incremental Datasets 48
Ji-Won Byun, Yonglak Sohn, Elisa Bertino, Ninghui Li

Privacy Preserving Data Management

Difference Set Attacks on Conjunctive Keyword Search Schemes 64
Hyun Sook Rhee, Ik Rae Jeong, Jin Wook Byun, Dong Hoon Lee

Off-Line Keyword Guessing Attacks on Recent Keyword Search Schemes over Encrypted Data 75
Jin Wook Byun, Hyun Suk Rhee, Hyun-A Park, Dong Hoon Lee

Privacy Preserving BIRCH Algorithm for Clustering over Vertically Partitioned Databases 84
P. Krishna Prasad, C. Pandu Rangan

Access Control

Conflict of Interest in the Administrative Role Graph Model 100
Yunyu Song, Sylvia L. Osborn

Two Phase Filtering for XML Access Control 115
Changwoo Byun, Seog Park

Hybrid Authorizations and Conflict Resolution 131
Amir H. Chinaei, Huaxin Zhang

Database Security

Analysis of a Database and Index Encryption Scheme – Problems and Fixes 146
Ulrich Kühn

Information Disclosure by XPath Queries 160
Stefan Böttcher, Rita Steinmetz

SPIDER: An Autonomic Computing Approach to Database Security Management 175
Hakan Hacıgümüş

Author Index 185