Lecture Notes in Computer Science 3674

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

## Editorial Board

Willem Jonker Milan Petković (Eds.)

# Secure Data Management

Second VLDB Workshop, SDM 2005
Trondheim, Norway, September 2-3, 2005
Proceedings

Springer

Volume Editors

Willem Jonker
Milan Petković
Philips Research Eindhoven
Information and System Security
Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands
E-mail:{Willem.Jonker,Milan.Petkovic}@philips.com

Library of Congress Control Number: 200593521

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-10 3-540-28798-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28798-8 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11552338 06/3142 5 4 3 2 1 0

# Preface

Although cryptography and security techniques have been around for quite some time, emerging technologies such as ubiquitous computing and ambient intelligence that exploit increasingly interconnected networks, mobility and personalization put new requirements on security with respect to data management. As data is accessible anytime anywhere, according to these new concepts, it becomes much easier to get unauthorized data access. Furthermore, 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 dynamic, context-aware, role-based), database security (e.g., efficient database encryption schemes, search over encrypted data, etc.), and privacy-preserving data mining to controlled sharing of data.

In addition to the aforementioned subject, this year we also called for papers devoted to secure data management in healthcare as a domain where data security and privacy issues are traditionally important. The call for papers attracted 38 papers both from universities and industry. The Program Committee selected 16 research papers for presentation at the workshop. These papers are also collected in this volume which we hope will serve you as a useful research and reference material.

The volume is divided roughly into four major sections. The first section focuses on encrypted databases addressing the topics of key and metadata management, as well as searching in the encrypted domain. The second section changes slightly the focal point to access control, which remains an important area of interest. The papers in this section deal with this topic from a different point of view and in a different context: two papers in the medical domain, one in the area of the Semantic Web and one in XML databases. The third section focuses on disclosure detection, control and prevention, again in a database environment. The last paper in this section addresses in particular the topics of inference control and anonymization in medical databases. Finally, the fourth section addresses privacy and security technologies which are required in a modern world to support concepts like ubiquitous computing or location-based services.

July 2005 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

Peter Apers, Twente University, The Netherlands
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
Eduardo Fernández-Medina, University of Castilla-La Mancha, Spain
Simone Fischer-Hübner, Karlstad University, Sweden
Tyrone Grandison, IBM Almaden Research Center, USA
Ehud Gudes, Ben-Gurion University, Israel
Marit Hansen, Independent Centre for Privacy Protection, Germany
Pieter Hartel, Twente University, The Netherlands
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
Stig Frode Mjlsnes, 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, KULeuven, Belgium
Jean-Jacques Quisquater, Universit Catholique de Louvain, Belgium
Kai Rannenberg, Goethe University, Frankfurt, Germany
Morton Swimmer, IBM Zurich Research Lab, Switzerland
Sheng Zhong, Stevens Institute of Technology, USA
Josip Zorić, Norwegian Telecom, Norway

## Additional Referees

Maarten Fokkinga, University of Twente, The Netherlands
Ling Feng, University of Twente, The Netherlands

Carlos Gutiérrez, STL, Spain
Jan Muntermann, Frankfurt University, Germany
Christiane Schweitzer, Karlstad University, Sweden
Maurice van Keulen, University of Twente, The Netherlands
Anna Zych, University of Twente, The Netherlands
Amit Jain, University of South Carolina, USA
Marcin Czenko, University of Twente, The Netherlands
Ha Tran, University of Twente, The Netherlands
Ari Saptawijaya, University of Twente, The Netherlands
Huiping Guo, George Mason University, USA
Erez Shmueli, Ben-Gurion University, Israel
Ronen Waisenberg, Ben-Gurion University, Israel
Claudine Conrado, Philips Research, The Netherlands
Djoerd Hiemstra, University of Twente, The Netherlands

# Table of Contents

## Encrypted Data Access



## Access Control



## Information Disclosure Control in Databases

## Privacy and Security Support for Distributed Applications