Lecture Notes in Computer Science 3178

Willem Jonker   Milan Petković (Eds.)

Secure Data Management

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

Springer

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

Springer is a part of Springer Science+Business Media

springeronline.com

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.

July 2004 Willem Jonker and Milan Petković

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

Privacy Preserving Data Management

Access Control

Database Security