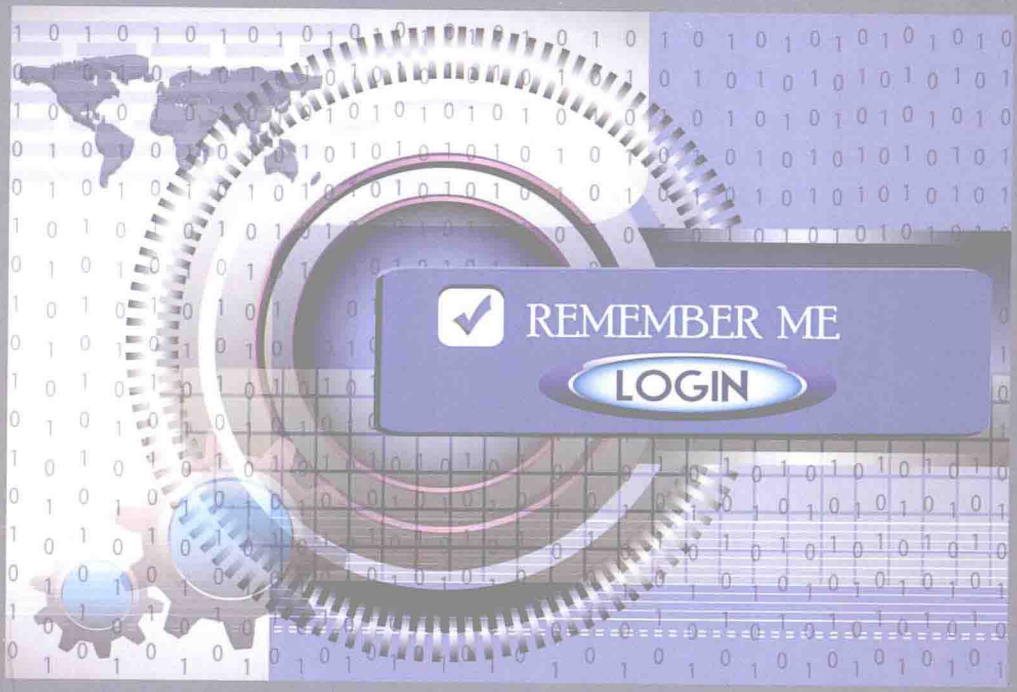
Multilevel Security for Relational Databases



Osama S. Faragallah
El-Sayed M. El-Rabaie • Fathi E. Abd El-Samie
Ahmed I. Sallam • Hala S. El-Sayed

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Multilevel Security for Relational Databases

Osama S. Faragallah
El-Sayed M. El-Rabaie • Fathi E. Abd El-Samie
Ahmed I. Sallam • Hala S. El-Sayed

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **Informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20140929

International Standard Book Number-13: 978-1-4822-0539-8 (Hardback)

Library of Congress Cataloging-in-Publication Data

Faragallah, Osama S.
Multilevel security for relational databases / Osama S. Faragallah, El-Sayed M. El-Rabaie, Fathi E. Abd El-Samie, Ahmed I. Sallam, and Hala S. El-Sayed.
pages cm
Summary: "Most database security models focus on protecting against external unauthorized users. Because multilevel secure databases provide internal security according to user access type, they are a viable option for the security needs of modern database systems. Covering key concepts in database security, this book illustrates the implementation of multilevel security for relational database models. It considers concurrency control in multilevel database security and presents encryption algorithms. It also includes simulation programs and Visual studio and Microsoft SQL Server code for the simulations covered in the text"-- Provided by publisher.
Includes bibliographical references and index.
ISBN 978-1-4822-0539-8 (hardback)
1. Database security. I. Title.

QA76.9.D314F37 2014
005.8--dc23 2014020608

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Multilevel Security for Relational Databases

OTHER TITLES FROM AUERBACH PUBLICATIONS AND CRC PRESS

Agile Strategy Management: Techniques for Continuous Alignment and Improvement
Soren Lyngso
ISBN 978-1-4665-9607-8

Anonymous Communication Networks: Protecting Privacy on the Web
Kun Peng
ISBN 978-1-4398-8157-6

Big Data, Mining, and Analytics: Components of Strategic Decision Making
Stephan Kudyba
ISBN 978-1-4665-6870-9

BYOD for Healthcare
Jessica Keyes
ISBN 978-1-4822-1981-4

C: From Theory to Practice
George S. Tselikis and Nikolaos D. Tselikas
ISBN 978-1-4822-1450-5

Creating and Marketing New Products and Services
Rosanna Garcia
ISBN 978-1-4822-0360-8

Disturbance Observer-Based Control: Methods and Applications
Shihua Li, Jun Yang, Wen-Hua Chen, and Xisong Chen
ISBN 978-1-4665-1579-6

Empowering Project Teams: Using Project Followership to Improve Performance
Marco Sampietro and Tiziano Villa
ISBN 978-1-4822-1755-1

Formal Languages and Computation: Models and Their Applications
Alexander Meduna
ISBN 978-1-4665-1345-7

How I Discovered World War II's Greatest Spy and Other Stories of Intelligence and Code
David Kahn
ISBN 978-1-4665-6199-1

Introduction to Software Project Management
Adolfo Villafiorita
ISBN 978-1-4665-5953-0

Intrusion Detection in Wireless Ad-Hoc Networks
Edited by Nabendu Chaki and Rituparna Chaki
ISBN 978-1-4665-1565-9

Network Innovation through OpenFlow and SDN: Principles and Design
Edited by Fei Hu
ISBN 978-1-4665-7209-6

Programming Languages for MIS: Concepts and Practice
Hai Wang and Shouhong Wang
ISBN 978-1-4822-2266-1

Security for Multihop Wireless Networks
Edited by Shafiullah Khan and Jaime Lloret Mauri
ISBN 978-1-4665-7803-6

Security for Service Oriented Architectures
Walter Williams
ISBN 978-1-4665-8402-0

The Art of Linux Kernel Design: Illustrating the Operating System Design Principle and Implementation
Lixiang Yang
ISBN 978-1-4665-1803-2

The SAP Materials Management Handbook
Ashfaque Ahmed
ISBN 978-1-4665-8162-3

The State of the Art in Intrusion Prevention and Detection
Edited by Al-Sakib Khan Pathan
ISBN 978-1-4822-0351-6

Wi-Fi Enabled Healthcare
Ali Youssef, Douglas McDonald II, Jon Linton, Bob Zemke, and Aaron Earle
ISBN 978-1-4665-6040-6

ZigBee® Network Protocols and Applications
Edited by Chonggang Wang, Tao Jiang, and Qian Zhang
ISBN 978-1-4398-1601-1

Preface

In this book we try to look at encryption-based multilevel database security through the eyes of database security researchers. Multilevel security for relational databases is an interesting information security topic. Most of the security models available for databases today protect them from outside, unauthorized users. A multilevel secure database provides internal security in relationship with the user's type of access to the database. A multilevel secure database system has been proposed to address the increased security needs of database systems. Researchers are in need of new algorithms in this area with their software implementation.

We summarize the main contributions of this book as follows:

1. This book is devoted to the issue of multilevel security in the relational database.
2. Multilevel security for relational database models is considered in this book, with a comparison between them using different evaluation metrics.
3. Modifications are presented to an existing multilevel security model in the relational database either to speed or to enhance performance.

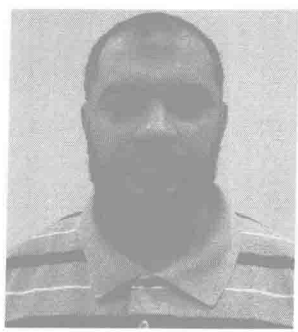
4. Formal analysis for data manipulation operations in multilevel security database models and mathematical proofs of soundness, completeness, and security are studied.
5. Simulation experiments are presented for validation of the discussed algorithms and modifications and also for investigating the performance of multilevel database models.
6. The C# and Microsoft SQL server source codes for most of the simulation experiments in this book are included at the end of the book.

Finally, we hope that this book will be helpful for database and information security.

About the Authors

Osama S. Faragallah received B.Sc. (Hons.), M.Sc., and Ph.D. degrees in computer science and engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He is currently associate professor in the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. He was a demonstrator from 1997 to 2002 and has been assistant lecturer from 2002 to 2007. Since 2007, he has been a member of the teaching staff of the Department of Computer Science and Engineering at Menoufia University. He is the co-author of about 100 papers in international journals, conference proceedings, and two textbooks. His current research interests include network security, cryptography, internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory.

El-Sayed M. El-Rabaie was born in Sires Elian, Egypt in 1953. He received a B.Sc. degree (Hons.) in radio communications from Tanta University, Tanta, Egypt in 1976, an M.Sc. degree in communication systems from Menoufia University, Menouf, Egypt in 1981, and a Ph.D. degree in microwave device engineering from Queen's University of Belfast, Belfast, U.K. in 1986. Until 1989, Dr. El-Rabaie was a postdoctoral fellow in the Department of Electronic Engineering, Queen's University of Belfast. He was invited to become a research fellow in the College of Engineering and Technology, Northern Arizona University, Flagstaff in 1992, and a visiting professor at the Ecole Polytechnique de Montreal, Montreal, QC, Canada in 1994. He has authored and co-authored more than 180 papers and 18 textbooks. He has been awarded the Salah Amer Award of Electronics in 1993 and the Best (CAD) Researcher from Menoufia University in 1995. He acts as a reviewer and member of the editorial board for several scientific journals. Professor El-Rabaie was the head of the Electronic and Communication Engineering Department at Menoufia University, and later, the Vice dean of Postgraduate Studies and Research. Dr. El-Rabaie's research interests include CAD of nonlinear microwave circuits, nanotechnology, digital communication systems, and digital image processing. He is a member of the National Electronic and Communication Engineering Promotion Committee and a reviewer of quality assurance and accreditation of Egyptian higher education.



Fathi E. Abd El-Samie received his B.Sc. (Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt in 1998, 2001, and 2005, respectively. Since 2005, he has been a member of the teaching staff in the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. He is currently a researcher at KACST-TIC in radio frequency and

photonics for the e-Society (RFTONICs). He is a co-author of about 200 papers in international conference proceedings and journals and 4 textbooks. His current research interests include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. In 2008, Dr. Abd El-Samie was the recipient of the Most Cited Paper Award from the journal *Digital Signal Processing*.

Ahmed I. Sallam was born in Tanta, Al Gharbia, Egypt in 1982. He received a B.Sc. degree (Hons.) in computer science and engineering from Al Azhar University, Faculty of Engineering in 2005 and an M.Sc. degree in computer science and engineering from Menoufia University, Faculty of Electronic Engineering, Egypt in 2012. He is a senior software engineer at Qarun Petroleum Company. His research interests include database, database security, cryptography, multimedia security, and image encryption.

Hala S. El-Sayed received her B.Sc.(Hons.), M.Sc., and Ph.D. degrees in electrical engineering from Menoufia University, Shebin El-kom, Egypt in 2000, 2004, and 2010, respectively. She is currently assistant professor in the Department of Electrical Engineering, Faculty of Engineering, Menoufia University. She was a demonstrator from 2002 to 2004 and an assistant lecturer from 2004 to 2010. Since 2010, she has been a member of the teaching staff in the Department of Electrical Engineering, Faculty of Engineering, Menoufia University. Her research interests are database security, network security, data hiding, image encryption, signal processing, wireless sensor network, robotics, secure building automation systems, and biometrics.

Contents

PREFACE xi

ABOUT THE AUTHORS xiii

CHAPTER 1 CONCEPTS OF DATABASE SECURITY 1
1.1 Database Concepts 1
1.2 Relational Database Security Concepts 5
1.3 Access Control in Relational Databases 7
1.3.1 Discretionary Access Control 7
1.3.2 Mandatory Access Control 10
1.3.3 Role-Based Access Control 12
1.4 Work Objectives 13
1.5 Book Organization 15

CHAPTER 2 BASIC CONCEPT OF MULTILEVEL DATABASE SECURITY 17
2.1 Introduction 17
2.2 Multilevel Database Relations 18
2.3 Polyinstantiation 19
2.3.1 Invisible Polyinstantiation 20
2.3.2 Visible Polyinstantiation 21
2.3.3 Types of Polyinstantiation 22
2.3.4 Architectural Considerations in Supporting Polyinstantiation 23
2.4 Multilevel Database Security Models 24
2.4.1 SeaView Model 24
2.4.2 Jajodia–Sandhu Model 26
2.4.3 Smith–Winslett Model 27

2.4.4 MLR Model 28
2.4.5 Belief-Consistent Multilevel Secure Data Model 29
2.5 Performance Study 30
2.5.1 Experimental Database Structure 30
2.5.2 Impact of Varying the Number of Tuples 31
2.5.3 Impact of Varying the Number of Attributes 31
2.5.4 Impact of Varying the Number of Security Levels 32
2.5.5 Analysis of Experimental Results 32
2.6 Summary 33

CHAPTER 3 IMPLEMENTATION OF MLS/DBMS MODELS 35
3.1 Introduction 35
3.2 SeaView Model 35
3.2.1 Selected Operation Procedure 35
3.2.2 Insert Operation Procedure 36
3.2.3 Update Operation Procedure 38
3.2.4 Delete Operation Procedure 38
3.3 Jajodia–Sandhu Model 40
3.3.1 Select Operation Procedure 40
3.3.2 Insert Operation Procedure 41
3.3.3 Update Operation Procedure 42
3.3.4 Delete Operation Procedure 43
3.4 Smith–Winslett Model 43
3.4.1 Select Operation Procedure 43
3.4.2 Insert Operation Procedure 44
3.4.3 Update Operation Procedure 46
3.4.4 Delete Operation Procedure 46
3.5 Multilevel Relational (MLR) Model 47
3.5.1 Select Operation Procedure 47
3.5.2 Insert Operation Procedure 48
3.5.3 Update Operation Procedure 50
3.5.4 Delete Operation Procedure 50
3.5.5 Uplevel Operation Procedure 52
3.6 Belief-Consistent Multilevel Secure Relational Data Model 53
3.6.1 Basic Procedures for Operations 53
3.6.1.1 Xview (Label) Procedure 53
3.6.1.2 Pl (Label) Procedure 55
3.6.1.3 Sl (Label) Procedure 56
3.6.1.4 Ib (Label) Procedure 57
3.6.2 Select Operation Procedure 57
3.6.3 Insert Operation Procedure 57
3.6.4 Verify Operation Procedure 59
3.6.5 Update Operation Procedure 60
3.6.6 Delete Operation Procedure 62

3.7 Comparative Study for Multilevel Database Models 64
3.8 Summary 64

CHAPTER 4 FUNDAMENTALS OF INFORMATION ENCRYPTION 65
4.1 Introduction 65
4.2 Basic Concepts of Cryptography 65
4.2.1 Goals of Cryptography 65
4.2.2 Principles of Encryption 66
4.3 Classification of Encryption Algorithms 67
4.3.1 Classification according to Encryption Structure 67
4.3.2 Classification according to Keys 68
4.3.3 Classification according to Percentage of Encrypted Data 70
4.4 Cryptanalysis 70
4.5 Conventional Symmetric Block Ciphers 71
4.5.1 Data Encryption Standard (DES) 71
4.5.2 Double DES 72
4.5.3 Triple DES 74
4.5.4 International Data Encryption Algorithm (IDEA) 74
4.5.5 Blowfish 75
4.5.6 RC5 Algorithm 75
4.5.6.1 RC5 Encryption Algorithm 75
4.5.6.2 RC5 Decryption Algorithm 76
4.5.6.3 RC5 Key Expansion 77
4.5.7 RC6 Algorithm 78
4.5.7.1 RC6 Encryption Algorithm 78
4.5.7.2 RC6 Decryption Algorithm 79
4.5.8 The Advanced Encryption Standard (AES) 81
4.6 Modes of Operation 83
4.6.1 The ECB Mode 83
4.6.2 The CBC Mode 85
4.6.3 The CFB Mode 85
4.6.4 The OFB Mode 86

CHAPTER 5 ENCRYPTION-BASED MULTILEVEL MODEL FOR DBMS 89
5.1 Introduction 89
5.2 The Encryption-Based Multilevel Database Model 90
5.3 Manipulation 92
5.3.1 The INSERT Statement 92
5.3.2 The DELETE Statement 93
5.3.3 The SELECT Statement 94
5.3.4 The UPDATE Statement 96
5.3.5 The UPLEVEL Statement 97

5.4 Performance Study 100
5.4.1 Experimental Database Structure 100
5.4.2 SELECT Query 102
5.4.2.1 Impact of Varying the Number of Tuples 103
5.4.2.2 Impact of Varying the Number of Attributes 104
5.4.2.3 Impact of Varying the Number of Security Levels 105
5.4.3 JOIN Query 105
5.4.3.1 Impact of Varying the Number of Tuples 106
5.4.3.2 Impact of Varying the Number of Attributes 107
5.4.3.3 Impact of Varying the Number of Security Levels 107
5.4.4 UPDATE Query 108
5.5 Analysis of Experimental Results 109
5.6 Summary 111

CHAPTER 6 FORMAL ANALYSIS FOR ENCRYPTION-BASED MULTILEVEL MODEL FOR DBMS 113
6.1 Introduction 113
6.2 The Encryption-Based Multilevel Model for DBMS Definition 114
6.2.1 MLR Model Definition 114
6.2.2 Encryption-Based Multilevel Model for DBMS Definition 115
6.3 Integrity Properties 117
6.3.1 Entity Integrity 117
6.3.2 Polyinstantiation Integrity 118
6.3.3 Data-Borrow Integrity 118
6.3.4 Foreign Key Integrity 118
6.3.5 Referential Integrity 119
6.4 Manipulation 119
6.4.1 The INSERT Statement 120
6.4.2 The DELETE Statement 120
6.4.3 The SELECT Statement 121
6.4.4 The UPDATE Statement 122
6.4.5 The UPLEVEL Statement 123
6.5 Soundness 124
6.5.1 Case 1: In the INSERT Operation 125
6.5.2 Case 2: In the DELETE Operation 125
6.5.3 Case 3: In the UPDATE Operation 126
6.5.4 Case 4: In the UPLEVEL Operation 126

6.6 Completeness 126
6.7 Security 128
6.8 Summary 131

CHAPTER 7 CONCURRENCY CONTROL IN MULTILEVEL RELATIONAL DATABASES 133
7.1 Introduction 133
7.2 Related Work 136
7.3 Enhanced Secure Multiversion Concurrency Control Model 138
7.4 Performance Evaluation 139
7.4.1 Workload Model 140
7.4.2 System Model 140
7.4.3 Experiments and Results 141
7.5 Correctness of the Enhanced Secure Multiversion Concurrency Control Model 143
7.5.1 Proof of Correctness 144
7.6 Summary 146

CHAPTER 8 THE INSTANCE-BASED MULTILEVEL SECURITY MODEL 147
8.1 Introduction 147
8.2 The Instance-Based Multilevel Security Model (IBMSM) 150
8.2.1 Definition 1: The Property View 151
8.2.2 Definition 2: The Class View 151
8.2.3 Definition 3: The Instance View at Classification Level L_j 151
8.3 The advant address of IBMSM 152
8.4 The Select Operation Procedure of the IBMSM 152
8.5 Insert Operation Procedure of the IBMSM 154
8.6 The Update Operation Procedure of the IBMSM 154
8.7 The Delete Operation Procedure of the IBMSM 157
8.8 Comparative Study for Polyinstantiation Models 157
8.9 Summary 159

CHAPTER 9 THE SOURCE CODE 161
9.1 Introduction 161
9.2 Screen Shots of the Prototype 161
9.3 Source Code of the Microsoft SQL Server 163
9.3.1 Source Code of the Data Security Classification Level Tables 164
9.3.2 Source Code of the User Security Classification Levels 166
9.3.3 Source Code of the Modifications to the Base Table 169
9.3.4 Source Code of the View for Each Model of the Multilevel Relational Database Models 174

9.4 Source Code of the Microsoft Visual Studio C# 185
9.4.1 Source Code of the Classes 185
9.4.2 Source Code of the Login Form 199
9.4.3 Source Code of the Queries Form 206
9.4.4 Source Code of the Query Form 232
9.4.5 Source Code of the Concurrency Control Form 259

REFERENCES 269
INDEX 277

1

Concepts of Database Security

1.1 Database Concepts

A database system is a computerized system whose overall purpose is to store and organize the data in a way that can be accessed, managed, and modified on demand. A database system becomes an important part of information management systems that enhances the ability of organizations to manage their important data in an easy way. A database system has many benefits that are described as follows:

- Reducing the amount of data redundancy by ensuring that the data are stored in one location and can be accessible to all authorized users
- Improving data access to users through use of host and query languages
- Enhancing data security
- Decreasing data entry, storage, and retrieval costs
- Allowing more flexibility for manipulating data
- Presenting greater data integrity and independence from applications programs

The interaction between the user, other applications, and the database itself can be performed through a software system called a database management system (DBMS) [1], which is specially designed to help the user to capture and analyze the stored data. The general purpose of the relational database management system is to be used as a tool to define, create, and manage the relational database.