MULTILEVEL SECURE TRANSACTION PROCESSING

The Kluwer International Series on
ADVANCES IN DATABASE SYSTEMS

Series Editor

Ahmed K. Elmagarmid

Purdue University
West Lafayette, IN 47907

Other books in the Series:

FUZZY LOGIC IN DATA MODELING, *Guoqing Chen* ISBN: 0-7923-8253-6

INTERCONNECTING HETEROGENEOUS INFORMATION SYSTEMS, *Athman Bouguettaya, Boualem Benatallah, Ahmed Elmagarmid* ISBN: 0-7923-8216-1

FOUNDATIONS OF KNOWLEDGE SYSTEMS: With Applications to Databases and Agents, *Gerd Wagner* ISBN: 0-7923-8212-9

DATABASE RECOVERY, *Vijay Kumar, Sang H. Son* ISBN: 0-7923-8192-0

PARALLEL, OBJECT-ORIENTED, AND ACTIVE KNOWLEDGE BASE SYSTEMS, *Ioannis Vlahavas, Nick Bassiliades* ISBN: 0-7923-8117-3

DATA MANAGEMENT FOR MOBILE COMPUTING, *Evaggelia Pitoura, George Samaras* ISBN: 0-7923-8053-3

MINING VERY LARGE DATABASES WITH PARALLEL PROCESSING, *Alex A. Freitas, Simon H. Lavington* ISBN: 0-7923-8048-7

INDEXING TECHNIQUES FOR ADVANCED DATABASE SYSTEMS, *Elisa Bertino, Beng Chin Ooi, Ron Sacks-Davis, Kian-Lee Tan, Justin Zobel, Boris Shidlovsky, Barbara Catania* ISBN: 0-7923-9985-4

INDEX DATA STRUCTURES IN OBJECT-ORIENTED DATABASES, *Thomas A. Mueck, Martin L. Polaschek* ISBN: 0-7923-9971-4

DATABASE ISSUES IN GEOGRAPHIC INFORMATION SYSTEMS, *Nabil R. Adam, Aryya Gangopadhyay* ISBN: 0-7923-9924-2

VIDEO DATABASE SYSTEMS: Issues, Products, and Applications, *Ahmed K. Elmagarmid, Haitao Jiang, Abdelsalam A. Helal, Anupam Joshi, Magdy Ahmed* ISBN: 0-7923-9872-6

REPLICATION TECHNIQUES IN DISTRIBUTED SYSTEMS, *Abdelsalam A. Helal, Abdelsalam A. Heddaya, Bharat B. Bhargava* ISBN: 0-7923-9800-9

SEARCHING MULTIMEDIA DATABASES BY CONTENT, *Christos Faloutsos* ISBN: 0-7923-9777-0

TIME-CONSTRAINED TRANSACTION MANAGEMENT: Real-Time Constraints in Database Transaction Systems, *Nandit R. Soparkar, Henry F. Korth, Abraham Silberschatz* ISBN: 0-7923-9752-5

DATABASE CONCURRENCY CONTROL: Methods, Performance, and Analysis, *Alexander Thomasian, IBM T. J. Watson Research Center* ISBN: 0-7923-9741-X

MULTILEVEL SECURE TRANSACTION PROCESSING

by

Vijay Atluri
Rutgers University

Sushil Jajodia
George Mason University

Binto George
Western Illinois University

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

Library of Congress Cataloging-in-Publication Data

Atluri, Vijay, 1956-
Multilevel secure transaction processing / by Vijay Atluri, Sushil Jajodia, Binto George.
p. cm. -- (The Kluwer international series on advances in database systems ; 16)
Includes bibliographical references and index.
ISBN 978-1-4613-7055-0 ISBN 978-1-4615-4553-8 (eBook)
DOI 10.1007/978-1-4615-4553-8

1. Database management. 2. Transaction systems (Computer systems) 3. Database security. I. Jajodia, Sushil. II. George, Binto, 1970- III. Title. IV. Series.

QA76.9.D3 A894 1999
005.4'34--dc21 99-047413

Printed on acid-free paper.

Contents

List of Figures ix

List of Tables xi

Preface xiii

1. INTRODUCTION 1
   1 Multilevel Secure Databases 2
      1.1 Why DAC is not enough? 4
      1.2 Additional Threats to Security: Covert Channels 6
      1.3 Multilevel Secure DBMS Architectures 8
   2 Advanced Database Application Domains 12
   3 Organization of the book 13

2. TRADITIONAL TRANSACTION PROCESSING 15
   1 ACID Requirements 15
   2 Concurrency Control Protocols 16
   3 Commit Protocols 18

3. TRANSACTION PROCESSING IN MLS DATABASES 21
   1 Problems with solutions in traditional environment 21
   2 Revised Requirements 23
   3 Commercial Solutions 24
   4 Research Solutions for Replicated Architecture 25
   5 Research Solutions for Kernelized Architecture 27
      5.1 Single version algorithms 27
      5.2 Multiversion algorithms 28
         5.2.1 Keefe-Tsai's scheduler 29
         5.2.2 Jajodia-Atluri's scheduler 29
         5.2.3 Snapshot Approaches 30
      5.3 Weaker Correctness Criteria 31
         5.3.1 Levelwise Serializability 31
         5.3.2 One-item Read Serializability 33
         5.3.3 Pairwise Serializability 34
      5.4 Using Transaction Analysis to Achieve Serializability 35

5.5 Multilevel Transactions 36
5.6 Secure Commit Protocols 37
5.6.1 Secure Early Prepare (SEP) 39

4. SECURE TRANSACTION PROCESSING IN REAL-TIME DATABASES 43
1 Introduction to Real-Time Databases 44
1.1 Priority Assignment Policies 47
2 Additional Requirements 47
2.1 Secure Priority Assignment 47
3 Concurrency Control 48
3.1 Real-Time protocols 48
3.1.1 2PL High Priority 49
3.1.2 OPT-SACRIFICE 49
3.1.3 OPT-WAIT 50
3.1.4 Performance Evaluation 50
3.2 Adaptive Secure 2PL (AS2PL) 52
3.3 Dual Approach 54
3.3.1 S2PL-WAIT 56
3.4 Secure Real-Time Two-Phase Locking Protocol 56
3.5 Fairness 59
4 Conclusions 61

5. SECURE WORKFLOW TRANSACTION PROCESSING 63
1 Introduction to Workflow Systems 64
1.1 Workflow Technology and Products 64
1.2 Workflow Product Categories 65
1.3 Workflow Standards 66
2 Workflow Transaction Model 67
3 Multilevel Secure Workflow Model 69
4 Solutions to Execute MLS Workflows 70
4.1 Semantic Classification of Task Dependencies in MLS workflows 71
4.2 Redesigning of MLS Workflows 75
4.2.1 Splitting the High Task: 75
4.2.2 Running a Compensating Task 76
4.2.3 Summary of the Redesigning Process 78
4.3 Alternative Solutions: Maintaining Multiple Versions: 78
5 The MLS WFMS Architecture 79

6. SECURE BUFFER MANAGEMENT 81
1 Introduction to Buffer Management 81
2 Requirements 82
3 Solutions 83
3.1 *-DBS Buffering System 84
3.1.1 Buffer Allocation 84
3.1.2 Replacement 85
3.1.3 Synchronization 85

3.1.4 Design Issues 86
3.1.5 Implementation 87
3.2 Performance Analysis 87
4 Secure Real-Time Database Buffer Management 88
4.1 Secure Buffering Algorithm for RTDBS 88
4.1.1 Security Features 89
4.1.2 Real-Time Features 89
4.1.3 Search and Slot Selection 90
4.1.4 Fairness Features 91
4.2 Performance Study 91
5 Conclusions 93

7. APPLICATIONS TO HIERARCHICAL AND REPLICATED DATABASES 95
1 Hierarchical Databases 95
1.1 Hsu-Chan Protocol 97
1.2 Ammann et al. Protocol 97
2 Replicated Databases 99

8. CHALLENGES 105
1 Using advanced transaction model paradigms 105
2 Secure Long Duration Transaction Processing 107
3 Recovery Methods 109
References 111

Index 123

List of Figures

1.1 Before the Trojan Horse Attack 5
1.2 After the Trojan Horse Attack 6
1.3 Example of a Covert Channel 7
1.4 The Integrity Lock Architecture 9
1.5 Vulnerability of The Integrity Lock Architecture 9
1.6 The Kernelized Architecture 10
1.7 The Replicated Architecture 11
1.8 The Trusted Subject Architecture 12
2.1 An incorrect concurrent execution 16
2.2 A correct concurrent execution 17
2.3 Basic 2PC Protocol 19
2.4 EP Protocol 20
3.1 A covert channel with two-phase locking protocol 22
3.2 A non-serializable history 22
3.3 The serialization graph corresponding the history in figure 3.2 23
3.4 A Crown 26
3.5 A multiversion schedule that can be generated by the Trusted Oracle 33
3.6 The distributed schedule *D* 38
3.7 SEP Protocol 41
4.1 Utility Function 45
4.2 Real-Time Database 46
4.3 Secure Priority Assignment 48
4.4 Secure Real-Time Concurrency Control 48
4.5 Adaptive Secure 2PL 53
4.6 MCC architecture for Dual Approach 55
4.7 Secure Real-Time Two-Phase Locking Protocol 57
4.8 GUARD Admission Control 59

5.1 Inter-level dependencies of the multilevel workflow transaction in example 1 70

5.2 Task dependencies in the MLS workflow in example 5.2 72

5.3 Modified Workflow after executing split task for example 5.1 76

5.4 An example demonstrating the closest ancestor 76

5.5 Modified Workflow after executing compensate task for example 5.2 78

5.6 Approach for redesigning each type of dependency 78

5.7 The MLS WFMS Architecture 80

7.1 An Example of Class Hierarchy in a Hierarchically Decomposed Database 96

7.2 A Planar Lattice 99

7.3 A crown-free DAG 101

7.4 Two forests produced by the DAG protocol on the DAG of figure 7.3 102

7.5 A DAG with crowns 103

7.6 A solution with a trusted node 103

7.7 A non-forest solution 104

List of Tables

5.1 A list of possible control flow dependencies 68
5.2 Some RD type dependencies and their inverse 77

Preface

Information security has been gaining a great deal of importance as computers are increasingly being used to process sensitive information. A *multilevel secure database management system* (MLS DBMS) is designed to store, retrieve and process information in compliance with certain mandatory security requirements, essential for protecting sensitive information from unauthorized access, modification and abuse. Such systems are characterized by data objects labeled at different security levels and accessed by users cleared to appropriate security levels. Unless transaction processing modules for these systems are designed carefully, they can be exploited by clever malicious users to leak sensitive information to unauthorized users.

Considerable research effort has been devoted since 1990 that has impacted the design and development of trusted MLS DBMS products. This book is a reflection of the progress and achievements made in this area. It covers the state-of-the-art of the research in developing secure transaction processing for popular MLS DBMS architectures: kernelized, replicated, and for distributed MLS DBMS as well as with advanced transaction models such as workflows, long duration and nested. Further, it explores the technical challenges that require future attention.

This book comprises of three logical parts. The first part of the book provides introduction and identifies the challenges in secure transaction processing. In particular, it gives an introduction to MLS databases including the different MLS DBMS architectures and an overview of traditional transaction processing approaches. It then identifies the desirable properties and the additional requirements imposed by multilevel security on transaction processing. It explains why conventional transaction processing techniques can conflict with the multilevel security constraints, discusses how they must be modified to comply with the security policy, and notes the challenges of doing so with acceptable responsiveness and with little or no trusted code.

The second part of the book provides secure transaction processing solutions for conventional databases. It examines the published solutions adopted by commercial vendors in their trusted DBMS products, that is, the extent to which they have succeeded in meeting the competing needs of multilevel transaction processing and efficiency. It presents secure concurrency control algorithms, based on locking and multiversion timestamp ordering, developed for replicated and kernelized trusted DBMS architectures, and provides an assessment of them. This book describes research in multilevel transaction correctness, where an individual transaction are able to write data at multiple security levels that leads to an additional trade-off between security and atomicity. It then discusses distributed multilevel secure DBMSs and describes the research on the impact of multilevel security on commit protocols for coordinating the execution of distributed transactions. Finally, this part discusses the impact of real-time constraints on secure transaction processing and reviews the research solutions in this area.

The third part deals with secure transaction processing in advanced application environments and more recent issues addressed. In particular, it discusses issues of transaction processing considering advanced transaction models such as workflow models and the buffer management issues in a MLS DBMS environment. It also presents the application of secure transaction processing solutions to hierarchical and replicated databases. Finally, the book concludes by identifying technical challenges in multilevel transaction processing that have yet to receive significant attention, including secure transaction processing using advanced transaction models such as nested and long duration models, and secure recovery.

This book is targeted towards researchers and developers in the area of multilevel secure database systems. It can also serve as a reference book for a graduate course on Database Security, Information Systems Security, Advanced Database Systems, and Transaction Processing.

Acknowledgments: The authors would like to acknowledge many contributors of this book. We thank the series editors, Ahmed Elmagarmid and Scott Delman, for their encouragement of this project, and Melissa Fearon of Kluwer for handling the logistics of getting the book through the publication process. We are grateful to Tom Keefe for his contribution to the section on recovery in chapter 8, Wei-Kuang Huang for allowing to use material from his dissertation in chapter 5, and Jayant Haritsa for his input to chapters 4 and 6. We also gratefully acknowledge the research funding of the National Science Foundation (IRI-9624222).