DETECTION AND PREVENTION OF MALICIOUS ACTIVITIES OFRELATIONAL DATABASE MANAGEMENT SYSTEMS (RDBMS)

ARAFAT MOHAMMED RASHAD ALDHOQM

A projectreport submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
University Technology Malaysia

JANUARY 2013

This project report is dedicated to my family (father, mother, wife, sons, daughter’sbrothers, sisters and uncles)fortheir endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisor Dr. MdAsri Bin Nagdifor his constant support during my study at UTM. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor.

Besides, I would like to thank the authority of University Technology Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

ABSTRACT

Insider attack is formsthe biggest threat against database management systems. Although many mechanisms have been developed to detect and prevent the misuse activities on the database systems, such as authorized modification on the approved records by the authorized users in malicious intent. However, thesemechanisms still have some limitations in detecting insider attacks. This study proposes a mechanism called dependency mechanism (DM) by utilizing the dependency relationship among database attributes to detect and prevent the authorized modification on approved database records, which have been already used, approved and closed by the system. The proposed mechanism is based on high and low dependency among attributes(columns). These dependencies based on the high and low repetition and usage of the attribute in the database. When the DM recognizes and detects any authorized modification on the approved records, it considers it as a malicious. The results of proposed mechanism DM showed high ability to detect and prevent the malicious modification on the approved records. Flag Based Mechanism (FBM) is considered as a baseline for this study. The evaluation parameter is a detection rate, by which the accuracy of the proposed mechanism is evaluated and compared to the FBM technique.

ABSTRACT

Serangan insider adalahancaman terbesarterhadapsistempengurusan pangkalan data.Walaupunbanyakmekanismetelahdibangunkanuntuk mengesan dan mencegahaktivitipenyalahgunaansistem pangkalan data,sepertipengubahsuaiandibenarkanpadarekodyangdiluluskan olehpenggunayangdibenarkandalamniat jahat. Walaubagaimanapun, mekanisme inimasihmempunyaibeberapa batasandalammengesanserangandalaman. Kajian inimencadangkansatu mekanismeyangdipanggilmekanismepergantungan(DM)dengan menggunakanhubunganpergantungandi antaraciri-ciripangkalan datauntuk mengesan dan mencegahpengubahsuaianyangdiberikuasapadarekod pangkalan datayangdiluluskan, yang telahsudah digunakan, yang diluluskan dan ditutupoleh sistem. Mekanismeyangdicadangkanadalahberdasarkankebergantungan yang tinggidansifat-sifatyang rendah di kalanganatribut (ruangan). Kebergantungan iniadalah berdasarkan kepadapengulangantinggi dan rendah danpenggunaanatributdalam pangkalan data. ApabilaDMmengiktirafdanmengesansebarangpengubahsuaiandibenarkanpadarekody angdiluluskan, iamenganggapiasebagaiberniat jahat. Hasildaripadamekanismeyang dicadangkanDMmenunjukkankeupayaanyang tinggiuntuk mengesan dan mencegahpengubahsuaianberniat jahat padarekodyangdiluluskan. MekanismeBenderaBerasaskan(FBM)dianggapsebagai asasuntuk kajian ini. Parameterpenilaiankadarpengesanan,dimanaketepatanmekanismeyang dicadangkandinilaidan dibandingkandengan teknikFBM.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ABBREV	**TITLE**
DM	Dependency Mechanism
FBM	Flag Based Mechanism
RDBMS	Relational Database Management System
DIDS	Database Intrusion Detection System
DEMIDS	Detection of Malicious Activities in Database Systems
SQL	Structure Query Language
PL/SQL	Procedural Language / Structure Query Language
DBMTD	Database Malicious Transaction Detection.

LIST OF APPENDIXES

CHAPTER 1

INTRODUCTION

1.1 Overview

Information is one of the main assets of any organization which is essential to its continuity. Therefore, information security is very important to protect the confidentiality, integrity and availability of the information. Many mechanisms and tools have been developed to protect the information systems from any possible incident such as access control systems, authentication systems, anti-virus software and firewalls.

According to Gong (2005), investigated different protection mechanism, whereit is impossible to have a completely secured system. Although sophisticated security systems can be used to achieve the information security requirements, however those systems may be under threats due to vulnerabilities or miss configuration of those systems. As a result, those vulnerabilities or missconfiguration may be exploited by intruders or implement their attacks. Therefore, Detection of Misuse Activities in Database Systems is considering as the last defence layer of the database security systems of any organization.The insider attacks formed the biggest threaten on the database systems due to an authorized access tothe database systems (Shatnwi et al. 2011). There are many types of insider attacks which try to abuse the access rights for example employees, masquerading and the malicious activities. Malicious activities are defined as a group of actions that attempt to threaten the Integrity and confidentiality of the database system (Heady, 1990). DEMIDS isa mechanism which hadbeen designed to detect and prevent the malicious activities on the database systems (Chung, 1999).

1.2 Problem Background

There are many insider attacks that may threaten the confidentiality, integrity and availability of database systems. According to Yushi et al.(2010) the database security attacks classified into two types of attacks such as outsider attacks and insider attacks. The outsider attacksmalicious action that causes many problems such as delay, bugs or damage. However, the insider attacks were categorized into legitimate and illegitimate access. Legitimate access can abuse the rights to do malicious actions, while , the illegitimate access exploits the vulnerabilities of the system to execute themalicious actions.

Many researchers have been conducting many studies of the insider attacks (Bertino et al., 2005). According to Shatnwi et al.(2011) the insider attack formed the biggest threaten on the database security level than the outsider attack because their knowledge about systems and their granted privileges.

Asmawi et al. (2008) indicated that the insider attacksformed the extremely dangerous on database systems. Furthermore, the insider attacks have rights to access database systems and doing maliciousactions. Dueto legitimate users, it is difficult to detect their malicious actions.

A malicious transaction is one of the insider attacks which is threatening integrity and availability of the database (Yushi et al., 2010). There are many reasons which are caused the malicious activities among them: bad configuration, low experiences of the Database administrator (DBA), hidden flaw and weakness of database implementation (Yushi et al., 2011).

Panda et al. (2003) stated that the mechanisms which have been developing based on auditing log filesonly detected the malicious commands, however the legitimate commands with malicious data havenot detected. Panda et al. (2003) proposed mechanism to detect the malicious activities in database system. The mechanism used data mining approach to determine the dependency among data attributes. The data dependency indicates to the access relations among data attributes. Itis generating in a set of rules (pre-written, read, and post-written sets). Therefore, the activities which have notfollowingtherules will detected as malicious activities.

The limitations of this mechanism are limited to user transactions that are matching to the read-write patterns which are assumed by author. Also, the system is not able to detect the malicious behaviors in individual read-write commands. Moreover, the false alarm rate may be more.Whilst same sensitive has been given to the each attributes, therefore there is no concept of attribute sensitivity (Bertino et al. 2005;Javidi et al. 2010).

Bertino et al. (2005) addressed thework of (Panda et al. 2003) by developing detection mechanismwhich is based on Role Based Access Control (RBAC) to detect the malicious behaviors. The techniqueswhich are using in this mechanism are working as control unit of the user role profile. If the techniques discovered that the user used different role instead of normal roles of user, will detected as malicious behaviors. This mechanism is suitable for databases that are employingRBAC model. The limitation of this approach is inability to detect the transaction level dependency, so some of the database attacks may be undetected (Rao et al., 2011).

Vieira et al. (2005) have developed Database Malicious Transaction Detection (DBMTD) mechanism to detect the malicious transaction based on predefined profile a transaction. Therefore, the transactionswhich are not matched with predefined transactions aredetected as misuse or malicious transactions. The limitations of this approach are limited transactions, profile manual generating,difficult to achieve it in the real database installations anddifficulty to determine the object level (Fonseca et al., 2008; Rao et al., 2011).

According to Aden Port Corporation R&D department (2003), Flag Based Mechanism (FBM) is one of the mechanisms which are introduced to detect and prevent the malicious transactions on the database systems. It has capability to detect the malicious behavior on the fly before committing in the database. Where, flag is a column in the database and responsible to determine the status of the records either approved or non-approved. The FBM has been implemented on the database of the Aden Port Corporation Since 2003 till now. The limitation of this mechanism is the DBA has capability to change the status of the flag from approved to non-approved easily.

Rao et al. (2011) haveaddressed the problem of Bertino et al.(2005) by developedmechanismwhich called Database Intrusion Detection System (DIDS).It has two phases: learning phase and intrusion detection phase. The learning phase generates authorized transactions profile automatically and the detection phase is checking the behavior of executable transactions by comparing it with authorized transaction profile. The limitations of this approach which are determined by researcher are difficult to capture the malicious data on authorized commands and difficult to determine the column level.

According to researcher, most of the previous studies have been developed to address the malicious transactions, however, unfortunately, most of them based on the database log files and auditing files to generate the authorized user profile which used to check the user behaviors.

This study proposed a new mechanism which is called Dependency Mechanism (DM). It based on dependency relationship among attributes to detect and prevent the malicious authorized modification on the approved records.

1.3 Problem Statement

One of the database security problems is insider malicious activities. For instance, modification is an insider malicious where record is approved by the authorized users. Existing mechanisms do not effectively address the severity of the modification on the approved records by authorized users. They based only on the predefined activities to detect the misuses behaviors. The problem statements emphasizing the goal of this study are: what is the required mechanism to detect and prevent the authorized modification on the approved records?

1.4 Project Aim

The aim of this project is to develop a new mechanism which called Dependency Mechanism (DM) based on dependency relationship among attributes to detect and prevent the authorized modification on relational database management systems RDBMS.

1.5 Project Objectives

The objectives of this project are:

i- To design a dependency mechanism to detect and prevent the authorized modification on the approved database records using dependency relationship among attributes.
ii- To develop the proposed dependency mechanism.
iii- To evaluate the dependency mechanism.

1.6 Project Scope

The scope of this project is limited on:

i- The proposed mechanism DM is limited only on the relational database management systems for the Aden Port Corporation.
ii- The proposed mechanism DM is limited only on the financial records.
iii- The dataset used is a real data of the database of Aden Port Corporation.
iv- The platform is limited on windows environment and developed by oracle9i database management, oracle9i developer2000, SQL* Plus and (PL/SQL) language only.
v- This mechanism is working on one of the insider attack categorization (Misfeasors).

1.7 Outline of Thesis

This study covers seven chapters. The chapters are organized according to different works that involved in this study. The detailed organization of this project is described in following paragraphs.

This **Chapter 1** describes a general outline of the project by giving a brief introduction of the project. The statement of the objectives and aims of the project were identified. The scope and importance of this project have also been pointed out. Hopefully this project will be successfully achieved by successful developing these objectives and aims of the project.

Chapter 2 establishes a background for the study and will begin by reviewing insider attack. This chapter also focuses more into the insider attack, its background, types and the categorization of the insider attack. Also, it focuses more about database modeling and dependency relationship. In addition to that the techniques and algorithms of the existing mechanism are analyzed. Finally it concludes the research findings from the literature review.

Chapter 3 demonstrates the methodology that has been used in this project. This includes project operational framework that describes all the different phases in the project.

Chapter 4 discusses the design of the proposed mechanism. Design includes the architecture, flowcharts and features and techniques of the proposed mechanism.

Results on the proposed mechanism will be discussed and compared with the previous existing tools in **Chapter 5**.

Chapter 6 is the conclusion of overall chapters and future works in the related area of the insider attacks. Also it includes recommendations for further study.

REFERENCES

Althebyan, Q. (2008). Design and analysis of knowledge-based centric insider threat models, ProQuest.

Asmawi, A., Z. M. Sidek, et al. (2008). System architecture for SQL injection and insider misuse detection system for DBMS. Information Technology, 2008. ITSim 2008.International Symposium on, IEEE.

Bertino, E., E. Terzi, et al. (2005). Intrusion detection in RBAC-administered databases. Computer Security Applications Conference, 21st Annual, IEEE.

C. Y. Chung, M. Gertz, et al :(2000) A misuse detection system for database systems.In 14th IFIP WG11.3 Working Conference on Database and Application Security.

Chickowski.E(2011).Insider Attacks and Human Error. Is Your Database Safe?http://www.channelinsider.com/c/a/Security/Insider-Attacks-and-Human-Error-Is-Your- Database-Safe-293745.

Codd, E. F. (1970). "A relational model of data for large shared data banks." Communications of the ACM **13**(6): 377-387.

Marczyk, G. R., D. DeMatteo, et al. (2010). Essentials of research design and methodology, Wiley.

Heady, R., G. Luger, et al. (1990). The architecture of a network-level intrusion detection system, Department of Computer Science, College of Engineering, University of New Mexico.

Fonseca, J., M. Vieira, et al. (2008). Online detection of malicious data access using DBMS auditing.Proceedings of the 2008 ACM symposium on Applied computing, ACM.

Shatnwi, N., Q. Althebyan, et al. (2011). Detection of Insiders Misuse in Database Systems. Proceedings of the International MultiConference of Engineers and Computer Scientists

Nguyen, N., P. Reiher, et al. (2003). Detecting insider threats by monitoring system call activity. Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, IEEE.Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics

Knüppel, R., P. Dietze, et al. (1994). "TRANSFAC retrieval program: a network model database of eukaryotic transcription regulating sequences and proteins." Journal of Computational Biology 1(3): 191-198.

Rao, U. P. and D. R. Patel (2011). "Design and Implementation of Database Intrusion Detection System for Security in Database."International Journal of Computer Applications 35(9).

Gong, R. H., M. Zulkernine, et al. (2005). A software implementation of a genetic Algorithm based approach to network intrusion detection. Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks.SNPD/SAWN 2005.Sixth International Conference on, IEEE.

Theoharidou, M., S. Kokolakis, et al. (2005). "The insider threat to information systems and the effectiveness of ISO17799." Computers &Security**24**(6): 472-484.

Vieira, M. and H. Madeira (2005).Detection of malicious transactions in DBMS. Dependable Computing, 2005.Proceedings. 11th Pacific Rim International Symposium on, IEEE.

Hu, Y. and B. Panda (2003). Identification of malicious transactions in database systems. Database Engineering and Applications Symposium, 2003.Proceedings. Seventh International, IEEE.

Yushi, A. and R. Bansal (2010). "Detection of Malicious Transactions in DBMS." international Journal of Information Technology and Knowledge Management, Julydecember**2**(2): 675-677.

Robert (2004)."Oracle Database 10g." www.ling.helsinki.fi/kit/2004k/ctl257/JDBC/Oracle-ch01-Intro.pdf

John Garmany (2002). “Easy Oracle PL/SQL Programming.” http://www.rampant Books.com/book_0501_easy_plsql.htm.

Briney, A. Prince, F. (2002), ‘ISM Survey 2002’, Information Security Magazine. http://infosecuritymag.techtarget.com/2002/sep/2002survey.pdf

DTI.(2002). ‘Information Security Breaches Survey 2002’. Department of Trade & Industry.

Einwechter, N. (2002).’Preventing and Detecting Insider Attacks Using IDS’, http://www.securityfocus.com/infocus/1558.

Neumann, P. G. and D. B. Parker (1989). A summary of computer misuse techniques. Proceedings of the 12th National Computer Security Conference.

Anderson, J. P. (1980). Computer security threat monitoring and surveillance, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.

Tuglular, T. (2000). A preliminary structural approach to insider computer misuse incidents. 1st European Anti-Malware Conference (EICAR 2000).

Schultz, E. E. (2002). "A framework for understanding and predicting insider attacks." Computers & Security 21(6): 526-531.

Phyo, A. and S. Furnell (2004). A detection-oriented classification of insider it misuse. Third Security Conference.

Port.(2003).http://www.portofaden.net/

Shawn,(2005).http://searchsqlserver.techtarget.com/definition/relational-database-management-system

Allan ,(2006).http://searchsqlserver.techtarget.com/definition/relational-database.

Cory ,(2006). http://www.techopedia.com/definition/1164/attribute-database-systems.