ALGORITHM TO PREVENT AND DETECT INSIDER MULTI TRANSACTION MALICIOUS ACTIVITY IN DATABASE

SEYYED MOJTABA DASHTI KHAVIDAKI

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

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

ABSTRACT

Almost all systems all over the world suffer from outsider and insider attacks. Outsider attacks are those that come from outside the system, however, insider attacks are those that are launched from insiders of the system. In this thesis is concentrated on insider attacks detection and prevention on the application level; database is our focus. Insiders have more knowledge about the underlying systems. Because of their knowledge and their privileges of the system resources; their risk can be greater and more severe. The insider execute multi transaction to inference the data, this is called multi transaction malicious. Several techniques have been proposed that tackled the insider multi transaction malicious problem, but most of them concentrate on insider threat detection in computer system level. We describe an algorithm for insider threat detection in database systems that handle multi transaction malicious activity. Our simulation results show resistance against multi transaction insider attack. Also, our results show good performance in terms of decreasing false alarms and increasing coverage detection.

ABSTRAK

Hampir semua sistem-sistem diseluruh dunia menghadapi penyerangan luaran ataupun dalaman. Penyerangan luaran adalah serangan dari luar sistem, manakala, penyerangan dalaman adalah serangan yang dijalankan dari dalam sistem tersebut. Di dalam kajian ini, ia lebih tertumpu kepada pengesanan penyerangan dalaman dan pencegahan pada tahap aplikasi; tumpuannya adalah pada pangkalan data. Orang-orang dalaman mempunyai ilmu pengetahuan yang mendalam tentang sistem-sistem asas. Oleh sebab mereka mempunyai ilmu pengetahuan yang mendalam dan juga mempunyai hak untuk mengakses sumber-sumber sistem; risiko tersebut adalah lebih tinggi dan teruk. Orang dalaman tersebut boleh menjalankan pelbagai transaksi untuk membuat gangguan pada data, ia dipanggil pelbagai transaksi berniat jahat. Beberapa teknik telah dicadangkan untuk menyelesaikan masalah ini, akan tetapi kebanyakan menumpukan perhatian mereka pada pengesanan ancaman dalaman didalam peringkat sistem komputer. Kami menerangkan algoritma untuk pengesanan ancaman dalaman didalam sistem-sistem pangkalan data yang boleh menangani aktiviti-aktiviti pelbagai transaksi berniat jahat. Keputusan simulasi menunjukkan penentangan terhadap penyerangan dalaman pelbagai transaksi. Selain itu, keputusan menunjukkan prestasi yang baik dari segi mengurangkan laporan yang palsu dan meningkatkan liputan pengesanan

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Everyone knows the significant of data which have special meaning to all of us and many people are involved with it in their daily life, such as using it in cost of products, account number, address of home, city post code etc. These examples show simple data to memorize, however some data cannot be memorized easily. As a result, these data and information should be stored in a special place to recall later. Different ways have used to reserve data, for example writing data on paper or engraving on rock which requiring a lot of time. Several technical methods and process for keeping data was designed by technology improvement such as database which is a data collection in a special arrangement and structure. Thus, it is an alternative providing opportunity to protect data.

Data protection is not only essentially important for some users like business users but also for nonprofessional's computer users. Since some events such as natural disaster and human behavior causing harms and much more cost, evaluating possible threats and susceptibility of system which is employed to protect the data should be taken into account. Therefore, securing data by using some new methods is a significant subject. In following, importance of data security is presented:

(i) Protection from of unauthorized data observation
(ii) Protection from unauthorized data modification

(iii) Security of the data confidential

(iv) Specific protection of integrity of data

(v) Verification of only data availability to authorized user

In order to preserve data with CIA (confidentiality, integrity and availability) deficiency which without them data can be destroyed or lost, database applications should be used. Thus, some novel techniques such as user authentication, user privileges, data encryption, auditing (Rathod *et al*.,2012), and etc. are suggested to protect data from mentioned damages. There are different types of attacks on database that is describe in Chapter 2; however intruder attack is a significant attack among them. Intruder attack includes two types' attacks named insider and outsider, whereas outsiders attack is more prevalent, so lots of Intrusion Detection Systems (IDSs) are designated to protect from it (Heights, 2009). To sum up, while a larger portion of attacks includes outsider attacks, but the insider tacks are more severe (Mun *et al.*, 2008).

Many studies prove that the "insider threat" is the most dangerous information security threat in advanced technological organization. The dangerous manner of user about database is principally the meaning of insider attack or it can be defined as "A person who has privileges to access the underlying system" (Nguyen *et al.,* 2003*).* In addition, insider is an individual who has the knowledge of the organizations information system structure to which he/she has authorized access" (a particular person knows the structure of organizations information system which has permission legally to access" is described as an insider). From (Maybury *et al.*, 2005) it can be inferred that workers employ their individual privileges to do actions on the basis of their information and have knowledge of some susceptibility of the system might be an insider and perform some attack. As a result, employee's attack has significant hazardous and critical effects (Nithiyanandam *et al.,* 2012).

1.2 Problem Background

Network, system, application and data are three different classifications of actions of insider threat. In classification of network, traffic activity is controlled through the intrusion detection system. However, intrusion detection systems (IDSs) perform action of checking in the system-level. Because of their importance application and data into account is taken. Several methods, algorithms and techniques with the aim of hindering and discovering activity of insider malicious are described here.

Misuse Detection-based on signatures (Gertz and Jajodia, 2007), Anomaly Detection-based on the behavior of the matter (Phyo and Furnell, 2004), A Detection-oriented approach classifies insider misuses based on the level of the system(Chung *et al.*, 2000). These three methodologies are explained to detect insider threat (IDS). In network and system level the ways of detecting and hindering insider threat are not efficient for data and application level (Shatnawi *et al.*, 2011).

To perform malicious transaction by attacker a novel technique named multi transaction is employed. By implementation of a database it becomes accessible to some user. Every application composed of a group of tasks that users have been allowed to apply a group of application. Within every task, at the end, a group of transactions are operated. Each task contains a series of transaction when users make a task definition to implement in database. The following items are background of multi transaction insider attack.

(i) The attacker can by alter the order of transaction because of having a group of them that execute as parallel, perform an attack on database, however each transaction can be executed in trusting way (Heights, 2009).

(ii) A user attempting to obtain or destroy unauthorized data from a database through aggregation and inference might retrieve more records than usual or have an abnormal data access pattern (Lee *et al.*, 2000).

Here is presented some methods and mechanisms with ability to find function of insider malicious. For hindering insider abuse action a model (an example or pattern) which is established upon user‘s task has been suggested by Yi Hu in (Heights, 2009). Only threat performs by individual task and model continue the functions of managing insiders is recognized by another insider misuse detector in database which suggested in (Shatnawi *et al*., 2011). In number of task that an insider can execute is limited. Also, detection of malicious task that include less than three transactions per task is weak. This model just tracks activity in order to control insiders. The insider‘s task in this pattern is restricted and obligated to determine purpose prior to action.

1.3 Problem Statement

The insider threat is the most important attack on database. A type of insider attack is malicious transaction. There are a few methods which are proposed to detect this activity. A new type of insider malicious transaction is multi transaction malicious activity. The insider executes two or more transaction or a task that include more than two transactions. This transactions are normal transaction but when execute together maybe do malicious activity or with running this task or group of transaction inference the data that has not permission to access to this data. Existing methods has some limitation or does not support this type of malicious activity. These limitations are listed below:

(i) Does not detect insider inference data.
(ii) Weak detection to detect multi transaction malicious activity.
(iii) Weakness of coverage percentage of detection

With regarding to the problem which mentioned before, the following objects are considered in this project:

(i) How to keep safe database system from malicious action?

(ii) How to prevent insider multi transaction attack?

(iii) How to detect insider multi transaction attack?

1.4 Project Goal

A model for finding and hindering misuse action is suggested since the database importance, misuse activity of insider and an effective mechanism shortage. Prevention process and detection process are two steps performed in this model. Firstly, this model examines functions of the users which are explained by users before executing and on the condition that the model finds transactions as a malicious transaction would be stopped. Second process observes work of user gradually and the transaction will not be cancelled unless any abuse is discovered. In addition, it does not have any requirement to explain purposed work before execute.

1.5 Project Objective

The Objectives of this study are as following:

(i) To investigate malicious activity on multi transaction in database.

(ii) To propose a malicious transaction detection and prevention algorithm to protect database.

(iii) To test the proposed detection and prevention algorithm on Sql server 2008 Ver 10.

1.6 Project Scope

Attacks cannot be recognized and restrained through the database software, so because of these, database software is selected. Database software that is most popular and most of organization and company use it to save their data. Sql server 2008 is the most popular in the both small and big company. Also Sql server 2008 support network, due to these the Sql server 2008 is selected. Also focus on detect and prevent malicious activity in database. Newest type of attack is multi transaction malicious activity and this thesis work on this attack, and prevent to inference data that has not allow to access it. Also the test doing by myself based on TPC-C benchmark standard that use university concept. The implementation of algorithm is done by C# 2010.

1.7 Project Significance

Since significant of information and growing rate of computer applications and information usages in present time this examination is worth a lot. Therefore, data and information in companies has more significant role. Moreover, it is essential to save information from destruction of privacy, integrity, and accessibility. Attacker attempts to obtain information and abuse them, thus a novel method to save data from insider multi transaction attack is required.

1.8 Organization of Report

This section is illustrated a highlights of this thesis. The project is based on six chapters that these six chapters are described in following paragraph. This section gives highlights the way different chapters are organized.

Chapter1 describe a general outline of the project by giving a brief overview and the problem of project. Statement of the objectives and aims of the project were presented. The scope and significant of the project have also states. The project will be successfully developing these objectives and aims of the project.

Chapter2 contains a history of database security and then a few database security terminologies. In continues, existing malicious transaction method was described. At the end information and limitation of existing algorithm were illustrate.

Chapter3 highlight the methodology operation framework. This framework consist three phases that are investigation, design, and evaluation. The first phase contains a literature review and presents a proposal as output of this phase. The second phase cover design the structure of algorithm. The last one is testing and evaluates the presented algorithm.

Chapter4 discuses and illustrates algorithm component by component. First of all describe a schema of algorithm and then describe specifically the algorithm. Both of two processes of algorithm that are detection process and prevention process are described with activity diagram and pseudo code.

Chapter5 focuses on algorithm implementation. Testing the algorithm was presented in this section. Parameter in testing and number of transaction that used in testing is described. At the end of section results between this algorithm and exist algorithm was compared and discussed.

Chapter6 looks at the conclusion and recommendation, as well as the judgment whether or not the objectives of the study are met.

REFERENCES

Ayushi., Sharma, A., Bansal, R. (2010). Detection of Malicious Transactions in DBMS. *International Journal of Information Technology and Knowledge Management.* 2(2): 675-677.

Barbara, D., Goel, R., and Jajodia, S. (2002). Mining Malicious Data Corruption with Hidden Markov Models. *Research Directions in Data and Application Security, Cambridge, England.*

Bertino, E., Terzi, E., Kamra, A., and Vakali, A. (2005). Intrusion detection in RBAC-administered databases. *Computer Security Applications Conference*, 21st Annual, IEEE, 10 pp.-182.

Chen, J., Lu, Y., & Xie, X. (2007). An Auto-Generating Approach of Transactions Profile Graph in Detection of Malicious Transactions. Intelligent Information Hiding , 1–4.

Chinchani, R., Iyer, A., Ngo, H., and Upadhyaya, S. (2005). Towards A Theory Of Insider Threat Assessment. *International Conference on Dependable Systems and Networks (DSN'05)*.

Chung, C. Y., Gertz, M., and Levitt, K. (2000). Demids: A misuse detection system for database systems. *Third International IFIP TC-11 WG11*. 5**:** 159-178.

Gertz, M., and Jajodia, S. (2007). *Handbook of database security*. Berlin: Springer-Verlag.

Hashemi, S., Yang, Y., Zabihzadeh, D., and Kangavari, M. (2008). Detecting intrusion transactions in databases using data item dependencies and anomaly analysis. *Expert Systems.* 25**:** 460-473.

Heights, H. (2009). Insider Threat in Database Systems : Preventing Malicious Users ' Activities in. 1616-1620.

Hu, Y., and Panda, B. (2004). A data mining approach for database intrusion detection. *Proceedings of the 2004 ACM symposium on Applied computing*. ACM, 711-716.

Hu, Y., and Panda, B. (2004). Mining Data Relationships for Database Damage Assessment in a Post Information Warfare Scenario. *Workshop on Information Assurance*. 401-409.

Javidi, M. M., Sohrabi, M., and Rafsanjani, M. K. (2010). Intrusion detection in database systems. *Communication and Networking.* Springer.

Karjoth, G. (2003). Access control with IBM Tivoli access manager. *ACM Transactions on Information and System Security (TISSEC).* 6**:** 232-257.

Lee, V. C., Stankovic, J. A., and Son, S. H. (2000). Intrusion detection in real-time database systems via time signatures. *Real-Time Technology and Applications Symposium*, 2000. RTAS 2000. Proceedings. Sixth IEEE . IEEE, 124-133.

Li, W., Panda, B., and Yaseen, Q. (2012). Malicious Users ' Transactions : Tackling Insider Threat. *Architecture*.

Maybury, M., Chase, P., and Cheikes, B. (2005). Analysis and Detection of Malicious Insiders Sara Matzner 1 . The Threat : Malicious Insiders Figure 1 . Heterogeneous and Multilevel Data Sources 4 . Event and Observable Taxonomy. Decision Analysis.

Mun, H., Han, K., Yeun, C. Y., and Kim, K. (2008). Yet Another Intrusion Detection System against Insider Attacks. *Proceesings, Symposium on Cryptography and Information Security*.

Nguyen, N., Reiher, P., and Kuenning, G.H. (2003). Detecting Insider Threats by Monitoring System Call Activity. *Workshop on Information Assurance.*

Nithiyanandam, C., Tamilselvan, D., Balaji, S., and Sivaguru, V. (2012). Advanced framework of defense system for prevetion of insider's malicious behaviors. *2012 International Conference on Recent Trends in Information Technology*, 434–438. doi:10.1109/ICRTIT.2012.6206788

Panda, B., and Zhou, J. (2003). Database Damage Assessment Using A Matrix Based Approach : An Intrusion Brajendra Panda and Jing Zhou. *Computer Engineering*. 1-6.

Parveen, P., Evans, J., Thuraisingham, B., Hamlen, K. W., and Khan, L. (2011). Insider Threat Detection using Stream Mining and Graph Mining. *IEEE International Conference on Privacy, Security, Risk, and Trust*

Phyo, A. H., and Furnell, S. M. (2004). A Detection-Oriented Classification of Insider IT Misuse. *Network Research Group.*

Raissi, D.M., and Carr, D. (2011). A multi-perspective approach to insider threat detection. *MILCOM 2011 Military Communications Conference*, 1164–1169. doi:10.1109/MILCOM.2011.6127457.

Rathod, Y.*A.,* Chaudhari, M.B., and Jethava, G.B. (2012). Database Intrusion Detection by Transaction Signature. *ICCCNT'12 26th_28th July 2012, Coimbatore, India,ieee.*

Sandhu, R., Ferraiolo, D., and Kuhn, R. (2000). The NIST model for role-based access control: towards a unified standard. *Symposium on Access Control Models and Technologies: Proceedings of the fifth ACM workshop on Role-based access control*. 47-63.

Shatnawi, N., Althebyan, Q., and Mardini, W. (2011). Detection of Insiders Misuse in Database Systems. *Computer*, I.

Srivastava, A., Sural, S., and Majumdar, A. K. (2006). Weighted intra-transactional rule mining for database intrusion detection. *Advances in Knowledge Discovery and Data Mining.* Springer.

Vieira, M., and Madeira, H. (2005). Detection of malicious transactions in DBMS. *Dependable Computing*. 350–357.