ABSTRACT

The recent rapid proliferations of web based applications with databases at its back-end have further increased the risk of database exposure to the outside world. Nowadays, there are many reports on intrusion from external and internal threats that compromised the database system. For that reason, it is important for us to provide protection for database systems from significant threats that comes from outside and inside the organizations. Currently, research on database security has been taken seriously as many solutions have emerged. All solutions should address the security elements that make up a lifecycle categorized into three areas which are prevention, detection and response mechanisms. This research focuses on the detection mechanism by deploying intrusion detection system (IDS) within the database management system (DBMS). The objective of this research is to propose a hybrid detection technique in order to cater external and internal threats which can provide protection for DBMS. This hybrid detection technique is called SQL Injection and Insider Misuse Detection System (SIIMDS). The technique combines the misuse and anomaly detection technique that consists of Misuse Detection Module, Anomaly Detection Module, Database Audit Log and Response Module. A prototype of the system was designed, implemented and analyzed to evaluate its security and performance. The analysis of the result in this research proved that the employment of this hybrid detection technique has provided better protection for DBMS in terms of high detection rates and low false alarm rates.

ABSTRAK

Perkembangan dalam aplikasi berasaskan jaringan yang mempunyai pangkalan data di dalamnya telah meningkatkan risiko pendedahan pangkalan data kepada dunia luar. Kini, terdapat banyak laporan berkenaan pencerobohan daripada ancaman luaran dan dalaman yang mengkrompomi sistem pangkalan data. Oleh sebab itu, penting untuk kita menyediakan sistem pangkalan data dengan perlindungan daripada ancaman luaran dan dalaman sesebuah organisasi. Kini, penyelidikan di dalam bidang keselamatan pangkalan data telah dijalankan secara serius dimana banyak penyelesaian telah ditemui. Semua penyelesaian harus mengambil kira elemen keselamatan yang menjadi satu kitaran hidup di mana ia dikategorikan kepada tiga bidang iaitu mekanisma pencegahan, pengesanan dan reaksi. Penyelidikan yang dijalankan ini akan memberi tumpuan kepada mekanisma pengesanan dengan menggunakan Sistem Pengesanan Pencerobohan *(IDS)* di dalam Sistem Pangakalan Data *(DBMS)*. Objektif penyelidikan ini adalah untuk mencadangkan satu teknik pengesanan hibrid untuk mengesan ancaman luaran dan dalaman di mana dengan penggunaan teknik hibrid ini akan meningkatkan perlindungan kepada *DBMS*. Teknik pengesanan hibrid ini dinamakan *SQL Injection and Insider Misuse Detection System (SIIMDS)*. Teknik ini menggabungkan teknik pengesanan penyalahgunaan dan teknik pengesanan kelainan yang mana ia terdiri daripada Modul Pengesanan Penyalahgunaan, Modul Pengesanan Kelainan, Audit Pangkalan Data dan Modul Reaksi. Satu prototaip sistem telah direka bentuk, dilaksanakan dan dianalisa untuk menilai keselamatan dan prestasi sistem tersebut. Analisis dari hasil penyelidikan ini telah membuktikan bahawa penggunaan teknik pengesanan hibrid ini telah menyediakan perlindungan yang lebih untuk DBMS dari segi kadar pengesanan yang tinggi dan kadar amaran palsu yang rendah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CSI	-	Computer Security Institute
DBMS	-	Database Management System
FBI	-	Federal Bureau of Investigation
HIDS	-	Host-based Intrusion Detection System
IDS	-	Intrusion Detection System
PHP	-	PHP Hypertext Preprocessor
SIIMDS	-	SQL Injection and Insider Misuse Detection System
SQL	-	Structured Query Language
URL	-	Uniform Resource Locator
VPN	-	Virtual Private Network
WWW	-	World Wide Web

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Preamble

The increasing development of information technology in the past few years has led to the widespread use of computer system applications in various public and private organizations such as banks, universities, manufacturing or service companies, hospitals, libraries, central or distributed administration. The increased reliability offered in hardware and software technologies coupled with the continuous reduction of costs, the increasing professional expertise of information specialists, and the availability of support tools, have all contributed to the widespread use of computing services. This implies that more data than ever is now stored and managed by computer system applications.

Information is a very critical asset in any organizations. Over the last few decades, it has become an organization's most precious asset and everything an organization does involves using information in some way or another, (Pepperd, 1993; Von Solms, 1993). Organizations use database systems and the information within them to automate various functions. These functions include payroll, inventory management and various types of forecasting and budgeting.

Today, more than just employees need access to data. It is important that partners and customers have access to the data as well. For that purpose, the data cannot simply be hidden behind a firewall because the partner and customer need to access the data for business transaction or data sharing. Therefore, it is important to secure the data from the threats and vulnerabilities of the outside world.

Korth and Silberschatz (1997) stated that the Web is, in effect, a large distributed database, albeit with a query language and access mechanism quite different from those traditionally included in a database system. Almost all computer system applications have the database management systems (DBMSs) at its back-ends as the main information sources. This information is considered as organization's most important asset and thus, need to be protected from rival companies or malicious attacks. They are stored in a database and managed by the DBMS. Therefore, it is challenge to ensure the confidentiality, integrity and availability of information held in these databases and database management systems. Due to its importance, information protection is a critical component of the database management system. Ones need to secure DBMS in order to protect the information stored in those DBMS.

In recent years the Internet connection has become a frequent point of attacks in most organizations. However, the loss due to internal attacks is far greater than the loss due to external attacks. According to Information Security Magazine survey done in

2002, 23% of respondents rated authorized users (insider) as their most important problem, while 11% reported unauthorized users (external hacker) as their most important problem (Briney and Prince, 2002). Similarly, results from the Department of Trade & Industry's Information Security Breaches Survey 2002 revealed that 34% of businesses considered their worst security incident to have been caused by an insider (DTI, 2002). Therefore, appropriate measures to protect information in database system from being exposed to the external hackers and misused by the authorized users are vital.

In line with the above view, this research focused on the detection of internal threats and external threats in database system environment to provide better level of security.

1.2 Background of the Problem

This section provides an overview of computer security problems and discusses issues related to database security, which is the focus of this study.

Castano *et al.* (1995) defined computer security as the protection of information processed by a computer against unauthorized observation, unauthorized or improper modification, and denial of service (ensuring no authorized use of the information is denied). Assuring computer to be in a secured status is not a trivial task since appropriate methods and tools are required for developing secure systems.

There is an increasing amount of research on database security. The reason behind this is that traditional security mechanisms, such as firewall could no longer work efficiently in today's environment. Web applications that are connected to the Internet make the DBMS that lie in the application becoming more exposed to attacks. Although in recent years, attacks from outside the organizations have increased due to increasing number of organizations getting connected to the Internet, insider attacks have also significantly amplified. Results from a series of Computer Crime and Security surveys conducted by Computer Security Institute (CSI) with the participation of San Francisco Federal Bureau of Investigation's (FBI) Computer Squad suggested that the dollar amount lost due to insider abuse is greater than the loss due to abuse from outsiders (Power, 2002). Therefore, protecting database system from both external and internal threats has become increasingly critical. According to Castano *et al.* (1995), the task of providing effective protection in database management system is particularly difficult, since they process large amounts of information in complex ways and require a fine granularity of control over data.

The general definition of database security is that it comprises a set of measures, policies, and mechanisms to provide secrecy, integrity and availability of data and to combat possible attacks on the system (threats) from insiders and outsiders, both malicious and accidental (Castano *et al.*, 1995). Data security, on the other hand, is defined as protecting information against unauthorized disclosure, alteration or destruction using hardware or software techniques (Feikis, 1999). Achieving security in a database environment means identifying the threats and choosing the proper policies ('*what*' the security system is expected to do) (Olson and Marshall, 1990); mechanisms ('*how*' the security system should achieve the security goals) (Bell, 1990) and the provision of security system assurance ('*how well*' the security system meets the protection requirements and executes the expected functions) (Andrews and MacEwen, 1990).

The mechanism of *'how'* the security system should achieve the security goals would be discussed in depth in this thesis. Feikis (1999) stated that the security mechanisms are functions used to implement the rules stated in the security policy. Security mechanisms can be divided into three categories: i) *prevention of improper access*, 2) *detection of improper access*, and 3) *recovery mechanisms*. For each category, there are many security mechanisms available. Each mechanism focuses on a specific kind of threat and deals with a specific form and aspect of security. Security mechanisms can be implemented via hardware, software or through administrative procedures. A security mechanism prevents a security violation from occurring during the operation; for example, a mechanism restricting physical access to a system (a locked door) or the use of access control mechanisms based on encryption to prevent unauthorized user from accessing objects. A detection mechanism ascertains attempted security violations, when or after they occur. Alarms can be used to detect unauthorized physical access. Audit trails can be used to detect unusual system activities after they have occurred. A recovery mechanism is used after a security violation has been detected. It restores the system to a pre-security violation state, e.g. backup tapes or redundant hardware.

The last element to achieve security in database environment is the security system assurance. According to Feikis (1999), system security assurance is used to provide consistency and integrity of the security mechanisms. These processes are intended to ensure that security recovery mechanism perform, as specified, under all workload and operating conditions. Feikis (1999) stated that database management systems have three major security issues of concern which are *confidentiality*, *integrity* and *availability*.

Confidentiality refers to information disclosure only to those users authorized to access it. The improper release of information caused by reading data from intentional

or unintentional access either observed or inferred is considered a breach of data confidentiality.

Integrity is the second security issue of database management systems. There are several areas of database integrity: *physical database integrity*, *logical database integrity* and *data element integrity*. Physical database integrity protection maintains data integrity through physical problems such as power failures and fires. Logical data integrity protection refers to the assurance that information is modified only by users entitled to do so. Maintaining data element integrity involves data accuracy and correctness.

The final issue is availability. This issue involves maintaining access to the database and all the data within the user's authorized domain. A denial-of-service attack involves actions that prevent users from accessing or using the database.

Threats to any of these categories are a breach of security and must be prevented. Consequences of these threats include improper exposure of information, improper modification of data, or denial of access to data and resources. The next section would discuss about current issues in database security which is SQL injection issue and insider misuse issue.

1.2.1 SQL Injection Issue

Most of the web-based applications that offer some kind of online services have a database at their back-ends. Such databases may contain sensitive information like credit card numbers, customer records, personal medical histories, banking transactions and commercial secrets. Any breach security to these databases can affect the reputation of the organization, loss of customers' confidence and might even result in lawsuits. Recent reports indicated that there is a large increase in the number of security breaches, which resulted in theft of transaction information and financial fraud (Poulsen, 2002; Atanasov, 2001; Hatcher, 2001). The hackers exploited poorly coded programs that interface with backend databases using SQL injection technique which is the most common attack upon web-based application (Spett, 2005).

SQL injection refers to a class of code-injection attacks in which data provided by the user is included in the SQL query in such a way that part of the user's input is treated as SQL code (Halfond *et al*., 2005). It is a trick to inject SQL query or command as an input possibly via web pages. They occur when data provided by the user is not properly validated and is included directly in a SQL query. By leveraging these vulnerabilities, an attacker can submit SQL commands directly to the database. This kind of vulnerability represents a serious threat to any web application that reads input from the users through web forms and uses it to make SQL queries to an underlying database. Most of the web based applications available on the Internet works this way and could therefore be vulnerable to SQL injection.

Before the web era, databases were protected by using the standard access control techniques such as Views and SQL authorization commands. Today, access control to web databases is implemented by applications and not by the database. Since the applications accessing the database can be very heterogeneous and their access

control can be very inconsistent, these can cause exposures to attacks from web applications. The number of attacks on databases has been increasing and it has become clearer that their access control mechanism is inadequate for web-based systems. The previous works proposed by other researchers to solve the SQL injection issue are discussed in Chapter 2.

1.2.2 Insider Misuse Issue

An internal threat is one in which someone with an authorized access to the organization could cause a loss to the organization if computer security went unchecked (Upadhyaya, 2003). The word authorized is a key term, as it emphasizes the main difference between an insider and external hackers. The perpetrators are those who work for the target organization or those having relationships with the firm with some level of access. It could be employees, business partners, contractors or even customers. Their motives could be in term of financial, social, political to personal gains. An insider should always be able to have at least a point of entry in one or more computer systems. The implications of having such a point of entry is that an insider does not usually need to consume as much time and effort to obtain additional privileges as an external hacker does, in order to exploit IT infrastructure vulnerabilities and mount an attack.

Phyo and Furnell (2004) had classified the insider misuse based on the level of the system at which they might be detected. The basis for this is the different types of misuses manifest themselves at varying levels of the system. Some may be apparent at network level, whereas others are most visible at higher levels, such as the operating

system, application and data levels. The previous works proposed by other researchers in order to solve the insider misuse issue are discussed in Chapter 2.

1.3 Statement of the Problem

A discussion on the background of the database security threats revealed the paramount importance of ensuring the security and privacy of information held in DBMS. DBMS as the main information sources need to be safeguarded against intrusions and insider misuses.

Current researches about intrusion detection and insider misuse have applied mature techniques to the computer networks, but they are limited in DBMS environment. For that reason, this study would focus on the deployment of intrusion detection for both external and internal threats in DBMS. The detection system would put consideration on both external and internal threats with respect to SQL injection and insider misuse attacks.

From the discussion on database threats, it is concluded that the data in DBMS is vulnerable from external and internal attacks. These attackers are everywhere and always-in '*ready*' position to compromised the DBMS. The main challenge in DBMS security is the ability to detect external threat from hackers while simultaneously detect internal threat from authorized users. Thus, it is crucial to take additional steps to ensure the confidentiality, integrity and availability of the data by implementing the

intrusion detection system for both external and internal threats. Based on this notion, the main statement of research problem is formulated as follows:

How to provide a better protection against SQL injection and insider misuses in DBMS environment?

An intrusion detection system (IDS) would be embedded within the database to provide a better protection against SQL injection and insider misuse. With the IDS as an additional protection, the DBMS would be more secure from external and internal threats.

1.4 Aim of the Research

The aim of this research is to propose a hybrid detection technique, which combined both anomaly and misuse detection techniques to provide protection for DBMS against SQL injection and insider misuse attack.

1.5 Objectives of the Research

The main objectives of this study are:

i) To study and analyze the existing techniques to provide better protection for DBMS.
ii) To design the SQL Injection and Insider Misuse Detection System (SIIMDS) which apply the hybrid detection technique based on misuse detection technique and anomaly detection technique.
iii) To implement the hybrid detection technique within the DBMS environment
iv) To evaluate the performance of the hybrid detection technique.

The research objectives stated above are expected to solve the problem statement of this research.

1.6 Scope of the Research

Since this research has inevitably some limitations, it was conducted within the research scope as described below:

i) The detection system would focus upon SQL Injections and insider misuse attacks in DBMS environment.

ii) The detection of the attacks would cater either SQL injection or insider misuse at one time.

iii) The detection system would be implemented using PHP scripts, MySQL database and Apache server.

iv) The detection system would be running on Ubuntu operating system and would be tested only in local host.

1.7 Organization of the Thesis

This thesis presents the general issues in database security, the specific issues in both external and internal threats upon database systems with focus on SQL injection and insider misuse attacks, and the detection method that would be employed in this study to counter both external and internal threats. This chapter has introduced the basic concepts in database security as a platform for the understanding of the research. The following is the outline of the thesis.

- **Chapter 2:** A detailed review on the body of knowledge related to database security is given. The review covers topic related to the database security and research issues focusing on SQL injections and insider misuse attacks in database system. The previous related researches particularly on intrusion detection system for DBMS are also discussed.

- **Chapter 3:** The chapter describes the research methods used in this study. The chapter starts with the introduction and followed by the discussion of each stage in the research methodology. The chapter ends with a summary.

- **Chapter 4:** Design and implementation of proposed intrusion detection system is given in this chapter. This chapter presents the SIIMDS system architecture, the algorithms development, system flow, SIIMDS component and SIIMDS software and hardware requirements.

- **Chapter 5:** This chapter presents the results and the evaluation analysis would on the performance of the system.

- **Chapter 6:** The discussion on the research contributions and conclusion of the thesis are given in this chapter. Recommendations and suggestions for future improvements are also covered.