Advanced Science and Technology Letters
Vol.107 (Ubiquitous Science and Engineering 2015), pp.38-41
http://dx.doi.org/10.14257/astl.2015.107.10

A Study on Detection of Malignant Query and Personal Information Leakage through Database Security Log Analysis

Gei-Young Kim[1], Kyung-Jin Jung[2], Yongtae Shin[3], Sangphil Kim[4] and Jong-Bae Kim[5*]

[1,2,3]Dept. of IT Policy and Mgmt., Graduate School of Soongsil Univ.,
Seoul 156-743, Korea
[4,5*]Graduate School of Software, Soongsil University, Sangdo-dong,
Dongjak-gu, Seoul, Korea
Corresponding Author: kjb123@ssu.ac.kr

Abstract. Many behaviors happen in information protection control, threatening from unauthorized change, destruction, and exposure to integrity, confidentiality, and availability of database, which is the final and core object of control. Like this it approaches database through numerous paths like many applications and home pages and execute query which search, modify, and delete the data. Some of it executes normal queries, but sometimes it maliciously executes the queries for leakage of information, and gives load to database server by executing the query which uses large amount of hardware resources. Traditionally it has limits, using only to find the reason for the problems, such as malignant queries, by collecting security log. Analyzing malignant queries and personal information leakage in diversified views through multidimensional analysis of data is necessary in order to use security log in more various ways. Therefore, this treatise is going to design multidimensional analysis modeling and suggest the technology to analyze in diversified views as an application plan of existing security log so that we can detect malignant queries and personal information leakage through security log analysis. We established the standard of analysis as follows for various analyses. First, we made linkage analysis available, which we cannot know with only simple history search, through analysis of database examination history. Second, we analyze if it repeatedly approached important table for a long time through detection of abnormal pattern or long term leakage via database abnormal access analysis. Third, we understood the flow of elements and data which weigh impact on specific database assets through database impact analysis and made analysis of database assets correlation and data flow analysis available. For analysis this treatise analyzed the log collected by using OLAP tools and used experiment data and operation data in order to verify the efficiency of database security log analysis technology suggested. Also we showed that the analysis method suggested by this treatise is excellent in availability and credibility in detection of malignant queries and personal information leakage, by comparing traditional data analysis method and the analysis method suggested by this treatise.

Keywords: Database Security, Log Analysis, Malignant Query, Personal Information, Detection

ISSN: 2287-1233 ASTL

1 Introduction

Database security is meant to protect external persons or insiders from leaking the important information assets of an individual or an organization. The treats to database security occur by user's mistake, misuse, and insider's abuse of his/her authority and/or attack to the known weakness of database. More and more threats occur to information assets saved and managed in database.

Since the existing database weakness analysis is initiated after accidents such personal information leakage by malicious query and system down by service overload, it is late and thus database can be exposed to an attack.

Therefore, the present study enabled to register database attack queries in Meta format and detect abnormal symptoms through multi-dimensional analysis on database audit history and abnormal access history in collected log files, which makes it possible to cope with potential attack to database in preemptive way.

2 Main Body

2.1 Types of SQL Injection Attack Queries

An intruder can use attack query to steal account information and password or create new account or password for the purpose of stealing the important assets in database by falsifying query internally in an abnormal way. The model proposed in the present study registers such attack queries by type and manages them in Meta format. Therefore, abnormal query can be instantly detected for judgment when security log analysis is conducted.

Table 1. Type of SQL Injection Attack Queries

Attack Type	Attack Query
Access to Table Name	Having 1=1
Access to Field Name	Group By
Access to Field Type	Union
Account Creation	Insert
Stealing Version and Configuration Information	@@Version
Account Extraction	Type Convert Error
Stealing Account Password	Union
DB Server Instance Down	Shutdown

2.2 Types of Personal Information Leaking Queries

Normally, personal information leaks out by insider's malicious intent or accidental mistake to leak database outside or by an external intruder's implantation of attack queries maliciously intended to leak out personal information. Many damages can bring out by personal information leakage: illegal use of other´s name, account stealing, voice phishing, SPAM mail, privacy risk. To prevent and minimize such damages involving with personal information leakage, the present study enables the proposed protection model to manage objects related to personal information, which is the starting point of personal information leakage, and analyze it by object.

2.3 Abnormal Pattern Detection Method

With patterns analyzed, it enables to detect unauthorized and abnormal access from a different band. It can identify information mapped differently by the flow of control target class to judge 'normal' or 'abnormal' access.

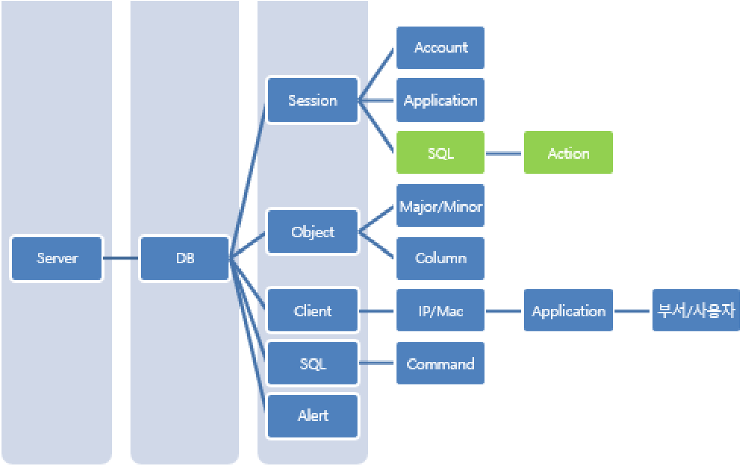

Fig. 1. Control Target Hierarchy

3 Conclusions

The proposed model demonstrated that it could collect database access control log data; analyze them; and detect abnormal patterns through DB audit history analysis and DB abnormal access analysis in a preemptive manner. In addition, the model was designed to handle and analyze bulky log data. Last, leakage analysis was possible: the connected analysis with other data than DB access control log data enabled to identify the factors that have an impact of the detection of malicious query and personal information leakage and this to reinforce security and manage DB assets.

References

1. Jong-Il Baek, Dea-Woo Park.: "A Study on DB Security Problem Improvement of DB Masking by Security Grade," Journal of the Korea Society Computer and Information, Vol.14, No.4, pp.101-109 (2009)
2. Bo-Man Lee, Dea-Woo Park.: "A Study on Intelligent Vulnerability DB Security System apply to Smart Grid," Journal of the Korea Society Computer and Information, No.44, pp.203-206 (2011)
3. Seungbae Choi, Changwan Kang, Jangsik Cho: "Behavior analysis of entrance applicants using web log data," Journal of Korean Data & Information Science Society, Vol.20, No.3, pp.493-504 (2009)