ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 133

2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE2016)

An Automatic Anti-Attack Scheme for MySQL Database

Qiao Sun[1], Lanmei Fu[1], Weihao Qiu[2] and Jiasong Sun[3,*]

[1]Beijing GuoDianTong Network Technology Co., Ltd., Beijing, China

[2]State Grid Zhejiang Electric Power Company, Hangzhou, China

[3]E. E. Department, Tsinghua University, Beijing, China

[*]Corresponding author

***Abstract*—Because of the high-speed, multi-user and multi-thread characteristics of MySQL database, it becomes one of the most popular open-source database. With the rapid development of network technology, SQL attacks against MySQL is also growing, and its security had been paid more and more attention. Due to the application of vulnerability SQL syntax inherent defects and MySQL, the attack to MySQL can get DBA access and download the database files, and even destroy the whole database system. Existing prevent MySQL attacks including many methods SQL attack detection, a front-end web server security agent, enhanced database authentication and encryption, enhanced database authorization and audit. But in practice, these methods still be unable to provide comprehensive MySQL anti-attack scheme for MySQL database, and generally reduce the network access speed. In this paper an automatic gateway deployment scheme, based on user permissions provide access between web server and database server, improve the MySQL database management system security through the management layer and business layer access control improved. The database security management scheme can be widely used in the national grid and other types of MySQL database security requirements of higher enterprise.**

Keywords-database management system security; MySQL attack; SQL attack detection; Automatic gateway deployment; user permission

I. INTRODUCTION

MySQL is developed by Oracle Corporation relational database management of open source platform, many network applications and project widely used MySQL as the default database system, its main advantage is can support multiple storage engine, support multi-thread/multi-users and support database cluster etc.. So it has been widely used in many personal user and enterprise user. But security of MySQL has been in academe and industry, developers must follow the code of the security technology, in order to restore the development of secure, robust and crack solution and application layer software must have the support of a security network and managed system, similar to the weak input validation (weak input validation such application layer vulnerability will lead to SQL injection attacks (injection attack) [1]. SQL injection is a development of Web application technology, in the use of the SQL query data provided by the customer before the removal of potential risk of attack. The existence of such a SQL injection vulnerability is easy for an attacker to execute arbitrary commands in database MySQL, such as access to sensitive information, tampering with data, and enhance the authority. Intrusion detection system plays an important role in protecting the security of computer systems and the Internet. It is a kind of active defense. Intrusion detection system can real-time detection of network status, monitoring network traffic, can also send out alarm, will record information to the database, and on this basis, the intrusion analysis generate intrusion log and audit data, effectively prevent the invasion of attack and to prevent a similar threat.

II. SQL DATABASE INJECTION ATTACK

Based on the SQL injection attacks are the most common way to attack database one of, the main reason is developers in the process of database design in the presence of defects that cause without filtering or the contents of the audit can be submitted to the database query code and data acquisition. Survey shows that in recent years, the global network based on the number of malicious software has significantly increased [2], while the global number of malicious software is one of the main reasons for the sharp increase in the number of injection attacks. At home and abroad to carry out research work to carry out the research work mainly [3]:

A. Coding Prevention

Code in the system useless full inspection of the contents of user input, so that hackers can be in the user can input place of injection attacks, the test of the database, and then attack. Therefore in the system implementation to be carried out to prevent the coding can be taken to prevent: the user input content for detection, the use of a common method of user input content coding, etc...

B. Static Analysis

Static analysis is a means to verify the content of the user input through the system, to detect whether there is a possibility of injection attacks. Or directly using the relevant tools to analyze, prevent injection attacks. However, the method needs to be combined with other methods to prevent injection attacks, and to prevent the injection attacks when used alone.

C. Based on Dynamic Pretreatment Statement

Dynamic pretreatment statement is in line with the requirements of the static syntax structure, defined in advance good logical structure to replace the original joint statement, by

pre statements on input sensitive character conversion, will lose the attack effect.

D. Context Sensitive String Evaluation

The method is to find the user input data, and the user input of any content to step by step verification, through the verification of the content that is legitimate data. Using this method to analyze the data, distinguish the data type, remove or replace the sensitive content.

E. Dynamic Analysis Tree

The principle of dynamic analysis tree is the reconstruction of the source code to form a new code, adding a user input parameters of the selection of non-sensitive information to the query statement, the same injection attacks to prevent.

III. INJECTION ATTACK DETECTION METHOD

At present, the commonly used injection attack detection methods in practical system include pattern matching pattern, expert system state and state transfer expert, etc.. In 1998, Roesch used Martin language to develop the open source intrusion detection system [4] Snort. Snort has developed into a multi-platform, real-time traffic analysis, network IP packet records and other characteristics of a strong network intrusion detection and defense system. Snort is based on misuse detection (Detection Misuse) of the network intrusion detection system [5], which is known to detect the threat behavior. It has a data capture data packet sniffer, charge from the network. Snort mainly consists of four parts: Data sniffer, pre-processor, detection engine log and alarm system. Read from the card data packets through pre-processor for processing, and then in the detection engine by rule detection data packet, if the packet with the rules will be disposed of in accordance with the rules, the overall structure of the as shown in Figure 1.

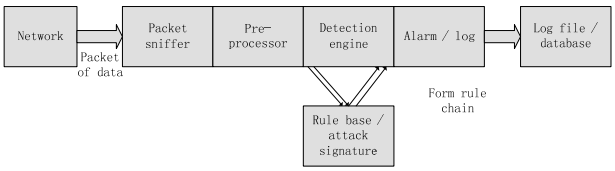

FIGURE I. SNORTIDS ARCHITECTURE.

In 1977, the BM algorithm as an efficient single pattern matching, an algorithm is presented [6], the basic idea is first on the pattern string P pretreatment and offset calculation of two offset function BadChar and GoodSuffix text string and pattern string alignment, matching each trip are from right to left of character by character comparison, when the text trip on character and pattern strings of characters do not match, reference function BadChar and GoodSuffix respectively, calculated as the value in both, as a text string pointer to the shift distance, if a tour match will be output.

In 1990, M.Sunday Sunday proposed the Daniel algorithm [7], whose idea is to consider the case of the next character of the text and the last position of the text when the offset array is calculated. Specifically, when the assumption $T[i] \neq P[j]$ does not match, at this time u has been matched to the part, and the length of the string u is assumed as L, the key of algorithm is based on the pattern of the u and $T[i+L+1]$ and the movement of the window. If the string $T[i+L+1]$ does not appear in the pattern P, this time mode $P[0]$ move to $T[i+L+1]$; if $T[i+L+1]$ appears in the $P[0]$, $T[i+L+1]$ start to search from the pattern on the right, if found and a character of the same in the $T[i+L+1]$ and P, $P[k]=T[i+L+1]$ is noted. At this time moving window make $P[k]$ and $T[i+L+1]$ align. And so on, until the completely matching.

IV. USING THE TEMPLATE AN ENHANCED AUTOMATIC ANTI-ATTACK GATEWAY DEPLOYMENT SCHEME

In order to improve the system of SQL to injection attacks resist ability, this paper puts forward a set of enhanced automatic anti attack gateway system deployment, as shown in Figure 2, through the safe management, including user DBA must through the security door to access or database management. Security door provides transparent proxy server, independent authorization management, attack protection, connection monitoring, log management and audit function. It controls the access port of the database firmly and enhances the security of database application. The main structure is that the transparent database security door is between the database server and the network server. It has 6 modules, including authorization, transparent proxy server, attack protection, connection monitoring, service settings and audit. The transfer between different modules is encrypted.

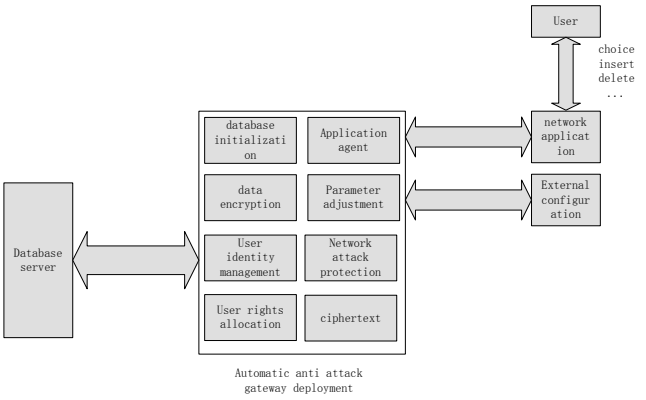

FIGURE II. NEW AUTOMATED ANTI ATTACK GATEWAY DEPLOYMENT SCHEME.

The main functions of these modules include:

A. The Authorization Module:

According to security access rules customized, authorization module will review the attempt to access the database user permissions. IP address, user name, database name, project name, form, and attempted to be combined into the authorized object. Some of the "IP address + users" object is authorized to the database of all services, so the security door

can be regarded as the database and the application of the separation of the virtual database.

B. The Transparent Proxy Server Module:

Application interface mapping technology, it can protect the IP address and port real database. The working mechanism of the module is similar to that of the traditional firewall system. Virtual database server IP, port and connection restrictions can also be set up.

C. Attack Protection Module:

It attacks real-time detection and defense of the different types of. When the user's operation has an attack code, the system can be identified in real time and automatically cut off the connection.

D. Connect Monitoring Module:

It real-time monitoring of all connections between server and connection information flow. If any unauthorized access or attack it will alarm and record in the log. Managers can interrupt a particular connection at any time, or review a particular connection with an audit module.

E. Audit module:

It provides audit function, including mandatory audit and general audit. The mandatory audit record important events, IP address of the attack Notes database connection and no access to unauthorized visitors, and. The general audit includes all SQL statements of the audit. All audit records will be recorded at the time, the audit file cannot be read or be rewritten.

F. Service Setting Module:

It provides a service management function set.

Among them, the attack protection module uses the network and database protocol analysis technology to analyze the received data packets, and then through the pattern matching algorithm to determine the legitimacy of statement SQL. The data packet acquisition module monitors the network and acquires the corresponding data packet, and the data packet is sent to the network protocol analysis module. Network protocol analysis module based on TCP/IP protocol to extract and reconstruct the information in the packet. The information will be sent to the database protocol analysis module. Database protocol analysis module will be extracted from the statement SQL and sent them to the SQL filter module. SQL filtering module application matching algorithm and the rules of the rules and they are compared to the rules of the library. Reaction module in the detection of intrusion to take measures. The system will cut off the connection between the TCP and the intruder. However, in most commercial applications, the application will break the intrusion detection system and route or firewall to prevent intrusion. SQL filtering is one of the core functions of the system. It analyzes statement SQL by comparing the application of the SQL access with the predefined access rules, to match the characteristics of the intrusion, and to accept the warning or record. Based on the type of intrusion, the system will improve its rules. Secondly, after receiving the statement SQL, the SQL filter module will be transformed into identifiable data, and check the legitimacy of the TCP and IP header data, as well as the use of pattern matching algorithm to check data.

We propose a new system pattern matching algorithm in attack protection module. The core content of the algorithm is to add pretreatment before Sunday algorithm. The initial pattern string P is divided into two parts, one is the head string, for a string of record mode on P of the long head of Make (len (head string) <len (P)); another is the foot string. Matching process is head_string and text string T matching, if the match fails and not at the end of the text, then in accordance with the head_string algorithm Sunday will move to the best possible location. Otherwise, try to match the foot_string to the corresponding position of the text string T. If this also fails, then the location of the head_string to the foot_string match failed position, and then has been matched to the end of the text string T. If this attempt is successful or at the end of the T, the matching process ends.

V. EXPERIMENTAL RESULTS

The experimental data set is Darpa 99 intrusion detection data set, the first 50, 100, 150, 200 rules were chosen as the rule of the resource database simulation. Secondly, the baseline BM algorithm (BM) and our algorithm are used to examine on this data set. The experimental results are shown in Fig.3. If the preprocessing of the algorithm is not considered, the number of string matching affects the time complexity of string matching. The worst case is when the head string in t[i] position successfully and the text string t match, so before I-1 characters match up the I-1, N-i+1，t[i] after the characters need and foot string match up the two, one is with foot string matching, another is in failure and foot string matching with the head string and new position re match. In the worst case, the improved Sunday algorithm is less than 2N times. So the time complexity of the improved Sunday pattern matching algorithm is O (2N).

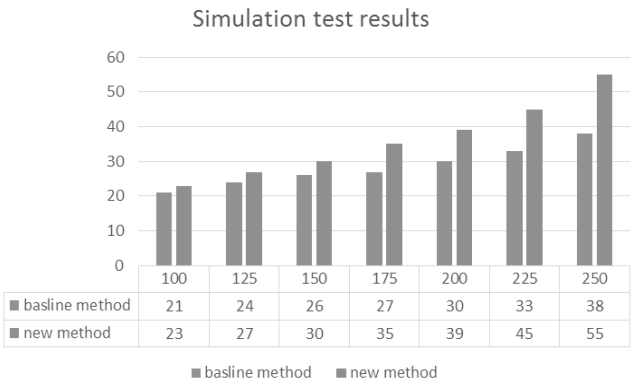

FIGURE III. SIMULATION TEST RESULTS OF TWO ALGORITHMS

After the establishment of two-dimensional chain, the filter. The filter module is used to establish a data packet structure after the SQL filtering module is obtained and the data packet is parsed, and the data in the structure is used to match the header information of the first Rule-Tree-Node in the vertical

direction. The return result of the matching function is "False", that is, the match fails, and the data in the data packet structure will match the next RuleTreeNode, until the end of the match. Join the return result is "True", then the data will be in the horizontal direction of the first OptTreeNode rule selection information matching. The next matching process is similar to that in the vertical direction. The value returned from the vertical and horizontal direction is "True", then the system detects an attack and will take a predefined measure. So from the whole point of view, the efficiency of this algorithm is more efficient.

VI. CONCLUSIONS

In this paper an automatic gateway deployment scheme, based on user permissions provide access between web server and database server, the improvement of the management and external business layer access control can improve the MySQL database management system security, the number according to library security management scheme can be widely used in electric power, finance, etc. the MySQL database type high security requirements of industry. Future work will include a combination of error detection and anomaly detection technology, so that we can reduce the false alarm rate and detect unknown attacks, and increase the accuracy of detection.

ACKNOWLEDGMENT

This research was financially supported by Science and Technology Project of the State Grid Corporation of China (SGZJ0000BGJS1500433) and the State Grid Information & Telecommunication Group CO.,LTD. (SGITG-KJ-JSKF[2015]0003).

REFERENCES

[1] D. Morgan, Web application security-SQL injection attacks [J], Network Security, vol. 2006, pp.4-5, April.2006.

[2] Liu Wenjin, SQL injection attack technology research in remote penetration testing [D], Master's thesis, Beijing Jiaotong University, 2009.

[3] Tang Zhengjun and Li Jianhua, Intrusion detection technology [M], Beijing: Tsinghua University press, 2004.

[4] https://www.snort.org/

[5] Zhu Yangchuan, Based on the analysis and design of Snort based telecom business security system [D], Master's thesis, Beijing University of Posts and Telecommunications, 2011.

[6] Qi Huiling, Pattern matching algorithm research and its application in the Snort system [D], Master's thesis, Southwest Jiao Tong University, 2010.

[7] D. M. Sunday, A very fast substring search algorithm [J], Communications of the ACM, vol. 33, pp. 132-142, Aug. 1990.