Available online at www.sciencedirect.com

SciVerse ScienceDirect

Physics Procedia 25 (2012) 1637 – 1641

Physics Procedia

2012 International Conference on Solid State Devices and Materials Science

Research on Intrusion Detection of Database based on Rough Set

Jihong Zhang,Xiaoquan Chen

Department of Computer Science,Transport Management Institue Ministry of Transport of the People's Republic of China,Beijing, China

Abstract

In this article, we apply the rough set theory to database intrusion detection and monitor the data in real time with intrusion detection. While theory based on rough set will judge the attacks according to the rules and respond to the sample data of intrusion detection after preprocessing them.

Keywords:rough set; intrusion detection; rule base; event generator

1. Introduction

The existing intrusion detection system is insufficient to set forth the concept of database intrusion detection system. They have neither taken into consideration structure and semantics, nor the exact granularity of datum in DBS. Microsoft SQL Server database security model can only achieve basic safe guard, while there is nothing it can do to all kinds of attacks on network. In this article, we study and design Database intrusion detection based on rough set and combining with intrusion detection technology. Intrusion detection based on Database rough set produces rule base, while event generator can monitor operations of database in real time, and event analyzer is used to confirm whether the operation is legal, suspicious or illegal. If it is a suspicious operation or illegal one, the event analyzer will sent the result to response units.

2.The system structure of database intrusion detection

MS SQL Server database security model is made up of the user, SQL login, limits of authority and tables. SQL Server classifies users into the following categories: database users, guest users, roles, database owners and the owners of database objects. Login method includes windows safe mode and

doi:10.1016/j.phpro.2012.03.287

hybrid safe mode. MS SQL Server database security model can realize basic safeguard, but it hasn't the ability to defend all sorts of attacks yet. After the intrusion detection is added to the database, once the event analyzer find any unusual action, MS SQL Server database security model will inform the response units. The system architecture of the database intrusion detection shows in figure 1. And it can be divided into DB, setting rules, rule base, event generator and response units.

2.1.Event generator

Realization resolution of event generator: first, we can use trigger mechanism to realize the generation. And then database Manage System tool can do it with audit tool, for example, event profiler of MS SQL Server 2000 or the management tool of SQL Server 2005 SQL Server Profiler can monitor the database. Event generator monitors the operation of the database in real time, and through the analysis the transaction of operation, it confirms the operating type and numerical value. Thus it transmits the analysis result to the event analyzer with certain format.

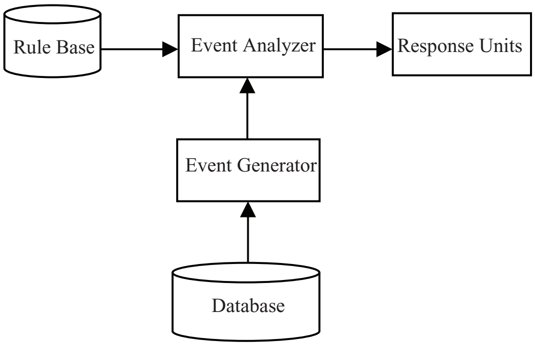

Fig. 1 Architecture of Database Intrusion Detection

2.2.Event analyzer

Event analyzer compares the operating transaction data with those are transmitted from event generator in certain forms with the rules in the rule base. It confirms weather it is legal operation, suspicious one or illegal one. If it is not the legal operation, the event analyzer will transmit the result to the response units.

2.3.Response units

Response units receive the analysis results from event analyzer. If response units ensure that the operation is suspicious or illegal, it will record the corresponding transaction information, the user of the operation, time, table and field and so on. And then, it gives out warning to the system administrator. As to the serious illegal operation, it will take the measures, such as disconnecting or disable Account.

2.4.Rule base

Extract the rule model with rough set theory, and pick up the characteristics of the users by analyzing the historic data, then conclude the regulation of the intrusion action, so that we can build up a more complete rule base for the intrusion detection. In a word, we can deal with broken datum and data dissociation with Rough Set Theory.

3.Database intrusion detection model based on Rough Set

Rule base in database Intrusion detection model based on rough set is mainly made up of three parts: data auditing preprocessor, RS brief, rule model. The database intrusion detection model shows in figure 2.

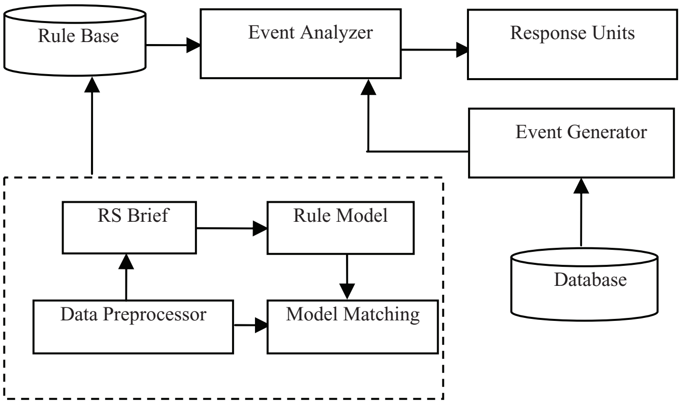

Fig. 2 Database Intrusion Detection Model based on Rough Set

Data preprocessor: dealing with or converting amounts of systemic auditing records. Because Rough Set is a notation analysis process, it's necessary to transform the systemic auditing records into symbol data and get a know-how table that's used to simplify the rough collections.

RS Brief: It comes to a simplified management using Rough Set Brief. The knowledge reduction deletes unrelated or unimportant attributes under the circumstance that the classification of knowledge base and decision-making ability are not changed. And then there forms a rule mode from the smallest attributes decision table which is get after simplification.

Rule mode: According different data types of the fields, we can set corresponding detection rule, including value A, value p and value q, we can set their upper limit and lower limit of their field values directly. What's more, one-way detection and both-way detection can also be set at the same time and the system will save the detection rules in the rule base in a certain format. Rule base can build a data table directly in the primary system database; rule base can also run in a certain format or file of expanded-name. These rules are the detection rule in the layer of word meaning, for example, numerical value boundary.

Systemic working process can be divided into two stages: practice stage and detection stage. In practice stage, in the basis of known normal auditing data and unusual auditing data, form the least rule mode after preprocessing and rough collection simplification. In detection stage, to the unknown normal auditing data, it's also necessary to classify the modes in the least rule modes after preprocessing. And at last, hand it over to the response units after the event analyzer has analyzed.

4.The application of the Rough Set in the Database intrusion detection model

In rough set theory, we call $S = \{U, A, V, f\}$ knowledge system. Among them, U stands for discussing domain of object, and A for attribute collection. $A=C\cup D$ Meanwhile A equals to all the different elements in C and D among which C stands for condition attributes collection and D for decision attributes collection. V_p is the value collection of collection p in collection A. f: $U\times A\rightarrow V$ is an information function.

As for knowledge system $S = \{ U , A , V , f \}$, B included in A is called binary relation, and $IND(B) =\{(x, y)\in U\times U \mid \forall p\in B，f(x, p) = f(y, p)\}$ is called unreadable in S. x and y is unreadable as to attributes collection B in S, if and only if f(x , p) = f(y , p) is right for all the elements in the collection p in which all its elements are in collection B.

Unreadable relation is an equivalence relation. Knowledge system $S = (U , A ,V , f)$ and $B \subset A$ can produce an equivalence relation of U. The ordered pair of *IND(B)* called $AS = (U , IND(B))$ is called approximation space. To any element x in U, the equivalence class of x in relation *IND(B)* can be expressed as $[x]_{IND(B)}$. The equivalence class of *IND(B)* is called base set.

Intrusion Detection sample datum constitute a knowledge system $S = (U , A , V , f)$ after preprocessing . The work of Rough Set knowledge reduction is to show the condition attributes of knowledge system and the dependence and relevancy decision attributes in the simplest way on the assumption of not losing information.

Attribute	Description
A1	protocol type
A2	source IP
A3	destination IP
A4	source location(EXTERNAL_NET, HOME_NET) etc)
…	…
A45*	dst_host_srv_diff_host_rate
A46*	dst_host_serror_rate
A47*	dst_host_srv_diff_host_rate
D	normal or special attack name

Fig. 3 Smallest Decision Rule Classification Model

We ask knowledge reduction not only for eliminating redundant information, reducing calculated amount, increasing the speed of identification, but preventing the loss of important information and the identification of validity because of the reduction. Generate condition parts of decision rule which are produced by the classification model of Rough Set through reduction about decision so that we can get a smallest decision rule classification model. Classification model shows in figure 3.

Build classification models:

- Basic attributes (28): A1 to A28;
- Set attributes (19): A29 to A47;
- Decision attributes: D.

Every rule of the rule base in this model is divided into two parts in logic: rule heads and rule options. Rule heads is made up of the operations, protocols, Source IP Address, Target IP Address and net mask and ports of the rule. Rule options includes alarm information and pattern information that needs monitoring. The general format of rule is:

<Rule operation> <protocols> <source host> <direction operator> <target host IP> <Destination Port> (<Rule Options one: value one>; <Rule Options two: value two>; …; <Rule Options number: value number>)

In front of parentheses is the rule head. In part in parentheses is the rule option. The phrase in front of a colon is part of rule Options section which is called option keywords. Rules option is not necessary to parts of the rules. it is only used to define the collection of specific characteristics of a particular packet.

The following is an example: alert tcp any any -> 192.168.1.0/24 100 (content:"|00 01 86 a5|"; msg: "mountd access";). The rule describes any use of TCP protocol to connect data packets of 100 ports on any host in network 192.168.1.0/24. If there is a binary data 00 01 86 a5, and “mountd access” will be issued as a warning, and data packets will be truncated according to required.

5.Conclusion

Rough set theory is applied to a database intrusion detection model in this article. Rough set theory based on audit data pre-processor, RS reduction, the rules in handling generates the rule base. The generator event transmits the operation transaction data of a certain format record. The event parser compares the operation transaction data and the rules of the rules database. If the operation is suspicious or illegal operation, the results of the event parser is passed to the response unit. We can set rule by database firewall in serious circumstances and prohibit access to specific users. And so it raises the detection rate.

References

[1] RAHMANZADEH V,GHAZNAVI-GHOUSHCHI M B.A multi-Gb/s parallel string matching engine for intrusion detection systems[M]//Communications in Computer and Information Science.Berlin:Springer,2008.

[2] KIM D Y,KIM S,CHOI L,et al.A high-throughput system architecture for deep packet filtering in network intrusion prevention[C]//Proc of International Conference on Architecture of Computing Systems.2006.

[3] SUSHANT S, FARNAM J, PATEL J M.WIND:workload-aware intrusion detection[C]//Proc of the 9th International Symposium on Recent Advances in Intrusion Detection.Berlin:Springer,2006.

[4] IHEAGWARA C,BLYTH A,SINGHAL M.A comparative experimental evaluation study of intrusion detection system performance in a Gigabit environment[J].Journal of Computer Security,2003,11(1).

[5] QIAN Yu-hua,LIANG Ji-ye.Combination entropy and combination granulation in rough set theory[J].International Journal of Uncertainty, Fuzziness and Knowlege-based Systems,2008,16(2):

[6] ZHU W.Topological approaches to covering rough sets[J].Information Sciences,2007,177(6).