Journal of Applied Science and Engineering Innovation, Vol.2 No.11 2015, pp. 435-438
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Research and Design on Multilevel Secure Database System

Xiao Zhang[1], Haiyan Zhao[1], Min Zhu[1], Ran Li[1], Jing Zhao[1]

[1] *Xi'an Communication Institute, Xi'an 710106, China*

Abstract: This paper introduces the design of multilevel secure database management system and offer relevant flow chart and core code, designed multilevel security secure database management access control module and accomplish the implementation of access control database module, expecting to provide some technical support for the future development of database.

Keywords data security; Implementation and Design; Multilevel Secure Database System; Access Control

INTRODUCTION

The concept of multilevel security dated back to the 1960s. US Department of Defense decided to seek some protection of confidential data computer at that time. Before that, there had been regulations to restrict the use of unauthorized persons access to confidential data within the computer, which is the so-called discretionary access control. For the systems with less demanding of security, discretionary access control is able to meet the security need. But in the applications on national defence or military and so on, due to the relatively high security requirements, we must Implement the mandatory access control. The database management system which implements mandatory access control is usually called Multilevel Secure Database Management System. The difference between it and ordinary database data multilevel secure database is that the data in MLS are given different security grades. At the same time, the database users are also given different security grades. Only the users with appropriate permissions have access the corresponding data.

BLP MODLE

The famous BLP model, proposed by Bel1.D.E and La Padula, is the first of a full, formal multi-level security model, and is the beginning of the study on computer security theory, and the MAC model mostly studied currently is the improvement, directly or indirectly, of BLP model.

BLP model puts forward the subject, object and the concept of their security level & non hierarchical range for the first time, this is the first complete math model strictly proved by formalization method on the system safety and widely used for describing the safety issue of computer.

BLP model provides the definitions for related subject, object, safety level function, condition, system and so on, defines 4 characters, proposes 10 theorems, designs 11 rules, gives formal representation and proves.

The subject in BLP model is defined as positive entity like progress; and the object is defined as negative entity like data, documents and so on; the subject-to-object access include: r(Read-only)、w(Read-write)、a(Add)、e(Execute).

Discretionary access control(DAC) and mandatory access control(MAC) consist of the BLP model's safety strategy. The DAC uses an access matrix, the element Mij means the access model from the subject Si to the object Oj, and the former can only access to the latter according to the access right in the access matrix. The MAC includes simple safety feature and some additional features, the system assigns safety level for all subjects and objects, includes their safety and range, and the system controls the subject-to-object access through comparing the safety levels of the two.

The BLP model is a state machine model, which formally define the conversion rules between the system, the system state, and inter-states. Moreover, the concept of security level is introduced in it and a set of safety rules is developed, with the purpose of limitation and constraint of the system state and the state transition rule. For a system, if its initial state is safe and the security feature is also maintained through a series of rules, it can be concluded that the system is safe.

In the BLP model, Each subject is given to a maximum security level and a current security level, and each object has a security level. The Subject has four access modes to the object: read-only(RO), write-only(WO), execute(E), read and write(RW), and the BLP model satisfies the following four characteristics:

(1) Simple security feature (ss-feature): When, and only when the security level Cs of a subject s dominates the security level Co of an object o, the subject s has only the "read" access to the object o.

s read o $\Longleftrightarrow$ Cs $\geqslant$ Co

(2) Asterisk security feature (*-feature): The subject s has the "write" access to the object o when and only when the security level Cs of the subject s is not greater than the security level Co of the object o, which can be characterized as

s write o $\Longleftrightarrow$ Cs $\leqslant$ Co

(3) Discretionary security feature (ds-feature): Each access must appear in the access matrix, which means that a subject can perform the appropriate access only when the required authorization be obtained.

（4）Compatibility: the object hierarchical level remains compatibility. The feature applies to the object’s tree form hierarchical structure, and the object’s safety level increases towards the leaf direction, its compatibility is with the operation system’s directory structure.

It can be seen that the ds-feature processes with discretionary access control and the ss-feature and the *-features process with mandatory access control. The permission of discretionary access control is determined by the owner of the object independently, while the permission of mandatory access control is determined by the specific security administrator, which is imposed by the system.

DEFECTS OF THE BLP MODEL

According to the axiom and rule of the BLP model, there are safety defects like the incompleteness of the safety level definition, the imperfection of the information, safety of the time domain,covert channel and so on.The existing safety defects include incompleteness of the information,

(1)The incompleteness of the safety level definition. The subject safety level includes a safety level and a range, confirm the current safety level when establishing subject, and keep it un-change during the whole life period of the subject. The method is much too strict and simple, also lack of flexibility.

(2)The imperfection of the information.BLP model applies to the rule of “Write up”, any subject could write the highest safety level data, and the highest write safety level is not limited; meanwhile as to some lower safety level data, the low safety level user could read but it doesn’t mean it could be rewrote by the lower safety level subject. Only the subjects in the stated write safety level range could rewrite so that the data integrity could be ensured. As for some high safety level subject, not all low safety level data could always be read.

The completeness level related to its safety level but not in corresponding sequence. If subject S with high safety level & low completeness level reads object O with low safety level & high completeness level, then the completeness of the latter would be damaged which is intolerant and shouldn’t happen.

(3)Poor availability of the BLP model. On one hand, the strategy of ”Read down, write up” could guard against the user with low safety level accessing sensitive information, on the other hand, it lowers the system’s availability by limiting the reasonable requirements that the high safety level user writes data to the non-sensitive object.

(4)Safety of the time domain. Time domain overlapping may occur when different subjects access to the same object, and sometimes leak information.

(5)Convert channel：no restrict for the inference and covert channel exists.

(6)There is a large access right for the trusted subjects because they won’t be restricted by the “*-feature”, and this doesn’t conform to the principle of minimum privilege.

ACCESS CONTROL MODES

Controlling access is a common means to carry out security strategies. Access Control includes discretionary access control and mandatory access control.

Discretionary access control is a commonly used access control strategy. It deals With users access to the data in the system according to their label and the access rules, the rules stipulate the user access to the data access patterns and the rule set implies the authorization information.

Discretionary access control strategy allows a user to grant other users access to authorization of certain objects. Users can make appropriate changes to the system parameters due to their own willingness. Here the "autonomy" means the owner of the resource may decide to access resources, and this access can dynamically transfer and recycling according to the principle of “work needs”. It’s commonly used to limit the data in the same security classification or the same range unauthorized flow. There are a variety of discretionary access control methods, such as power meter, passwords, access control lists, etc.

Mandatory Access Control is a powerful access control means. The strategy restrict user’s access to information in the dependence of objects and subjects of the security level, assigning localized security level to users and data, then the system will take use of the security data to decide whether the user can have access to some resource. This way of access control is also called assignation access control mode. The so-called "assignation" refers to the access to resources is not determined by the owner of the resource but the security manager of the system, usually used to restrict the data flow from a high security grade to a low one, from a range to another, which can guarantee the confidentiality and integrity of the system.

DESIGN OF SYSTEM

The system adopts three structure layers. The top layer is the user service layer and it provides a friendly interface for users to browse information. The middle layer is the application layer services, which provides standard database access for database applications and controls the access to database, being completed by the database proxy server. The lowest layer is the data service layer, using the function of data definition, storage, backup and retrieval and it is completed by the database server.

In order to meet the needs of secure access and introduce database security proxy, the system can be divided into client and database security proxy. The client proxy includes application program interface module and communication surface module. Database security agent comprises a communication interface module, and requests analysis module, accessing and inferring control module control module, audit module and proxy access module. The system architecture is shown in Figure1.

The application program sends user's requests and the user's identity information through the client interface. Firstly, the database agent analyzes the query request when receiving the news, through the SQL analytic and transfer to the discretionary access control module. When discretionary access control check passes, the user access request is transmitted to the mandatory access control module for mandatory access check. After compulsory access control checks, user access request will be transmitted to the inference control module, checking whether the user can reason out unauthorized information according to information obtained by this visit and prior knowledge. If the reasoning control is checked by inspection, the user is allowed to target the database access module through a proxy, or he/she will be informed that the client that access is denied and disconnected. Whether the user can make it, the audit module will still records.

Database security proxy is bridged between the applications and the database, which plays a role of database middle ware. Agent system provides a standard database access interface for the database applications and manages the requests for the access to the database, which completely overcomes the disadvantages of traditional client/server model and has the advantages of good reusing and managing, flexibility and easy maintenance etc.

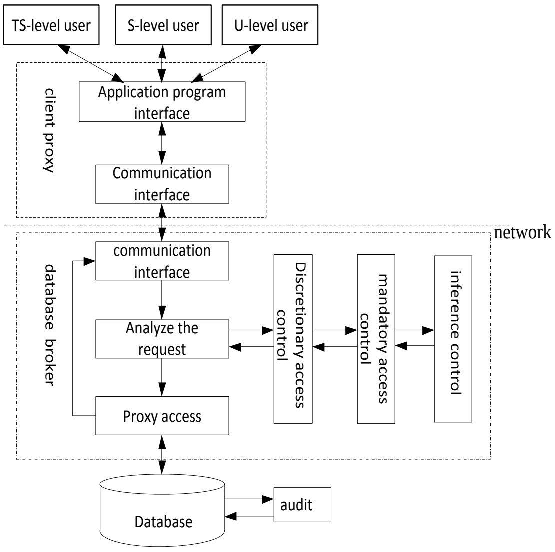

Figure 1 System architecture related modules schematic diagram

SYSTEM IMPLEMENTATION

System processes as shown in figure2.

Firstly the system will initializes, treatment process begins processing the information, which is sent by the client. If the information received is the end, the process is finished. If the operation is a user's request information database, the request analysis module is called to analyze the user request, then the analysis results and the user identity information will pass to control module, if the access control checks do not pass, then the user is returned to refuse query information and ends the process. If the access control checks pass, the information will be transmitted to inference channel control module, after the channel control module detects, decision results obtained. Results are divided to allow access and deny access, if it is allowed access, the database of user information will transmit to proxy access module. The module will be completed by proxy access module. If it is denied access, client sends denied information to users and ends the treatment process. Whatever the outcome, the audit module should be recorded, when audit module discovered an illegal operation, the audit module will terminate users access and alarm.

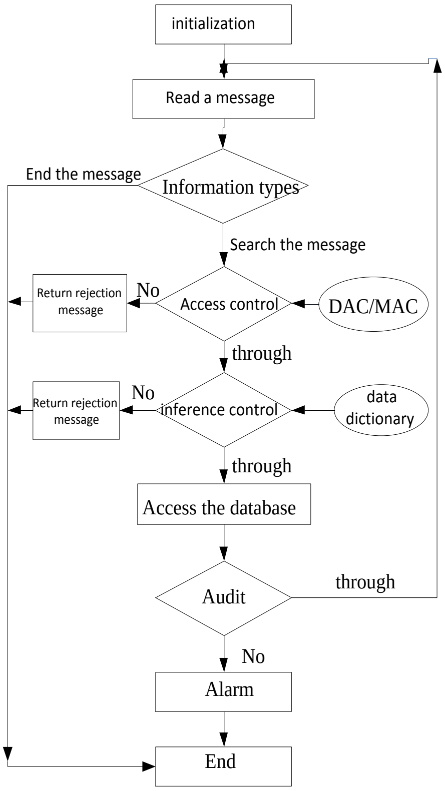

Figure 2 The flow chart of the system

CONCLUSION

Multilevel secure database management system has been researched by a large number of foreign researchers. Although the multilevel secure database prototype system in many high security has been achieved, there are many problems which have not been solved yet. This paper introduces the design of a multilevel secure database management prototype system, completing the system structure. We sincerely hope that this research can provide some technical supports for the database development in the future.

ACKNOWLEDGMENT

This work is supported by the National Science Foundation of China(61179002), Shaanxi Natural Sciences Foundation(2011JM8030).

REFERENCES

A Evfimievsk, J Gehrke, R Srikant. Limiting privacy breaches in privacy preserving datamining [J] . In Proceedings of the 22nd Symposium on Principles of Database Systems, ACM Press, 2003: 211- 222

Hinlce Thomas H.InIerence Aggregation Detection in Database Management Systems[C]. In:Pro IEEE Symp Research in Security and Privacy, Oakland, CA, New York. 1988:96～106

J Domingo- Ferrer. Advances in inference control in statistical databases: An overview in inference control in statistical databases: from theory to practice [J]. LNCS2316, Springer- Verlag, 2002:1-7

Jajodia S, Meadows C. Inference problems in multilevel secure database management systems[A]. Abrams M, Jajodia S, Podell H, eds. Information Security: An Integrated Collection of Essays[C]. Los Alamitos: IEEE Computer Society Press, 1995，570-584

L Wang, D Wijesekera, J Sushi.l Cardina lity-based inference control in sum - only data cubes[J]. In Proceedings of the 7th European Symposium on Research in Computer Security, 2002

S R izv,i JH aritsa. Maintaining data privacy in association rule mining[J]. In Proceeding s o f the 28th International Conference on Very Large Data Bases, 2002: 682- 693