Design and Implementation of Multilevel Secure Database Management Access Control

Haiyan Zhao[1], Mingshun Xing[1], Jing Zhao[1] and Hui Li[1]

[1] Department of Network service, Xi'an Communication Institute, Xi'an 710106, China

Abstract：This paper thoroughly analyzed the discretionary access control and mandatory access control, 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 *D*ata security; Access Control; Multilevel Secure Database Management

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.

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.

ACCESS CONTROL IMPLEMENTATION

The access control system uses a combination of discretionary access control and mandatory access control.

Discretionary Access Control Design

The user's access request will be passed to the discretionary access control module after analysis and interpretation. Then discretionary access control module will check whether the user has permission to perform operations such as the insertion of the class. If passed discretionary access control check, the user's access request will be conveyed to the mandatory access control module, otherwise it will be denied.

The system analyses the access request from the users and obtain the access subjcet, object and operation type. The subject is obtained from the permission control when the users are loging in while operation type is obtained according to the user's access request. The obtainment of the object can be generally divided into two situations: There exist

explicit access objects in the access requests, the access object can be obtained directly; when there is no explicit access objects in the access requests, you need to make an access change, obtaining the access object through accessing the database and constructing a triple<subject, object, access type> according to the returned result. Afterwards, judge if the access permissions of each triplet meet s the need according to the safety relational tables. Only if all the triplets meet the need of access requests can be controlled through discretionary access control, otherwise the access request will be rejected.

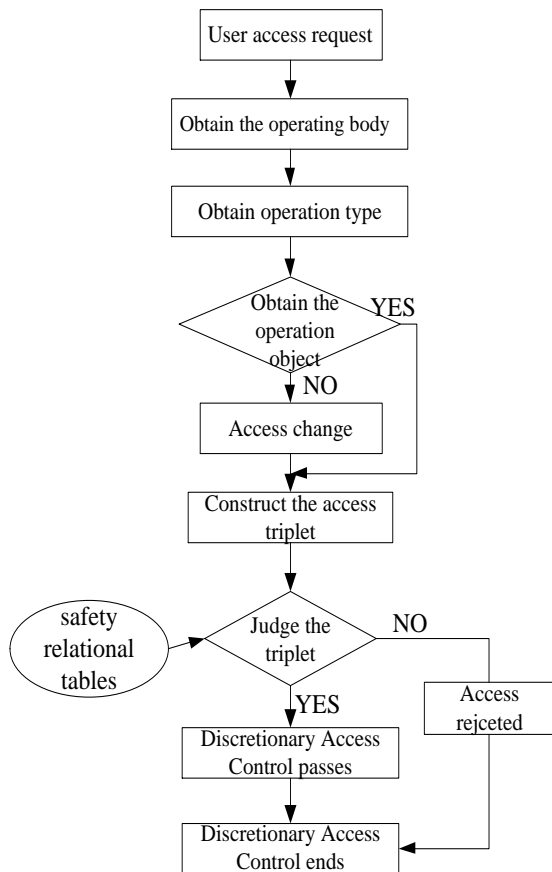Discretionary Access Control implementation flowchart is as shown in Figure1.

Figure 1.Discretionary Access Control implementation flowchart

Mandatory Access Control Design

After the system passes the access control check, it starts to conduct Mandatory Access Control. First, obtain the security grades and ranges of the subject and object.

Then check access control rules of the tuple in accordance with the application model access rules. If all the tuples satisfy the access request, it can be controlled through Mandatory Access Control, otherwise this access request will be rejected.

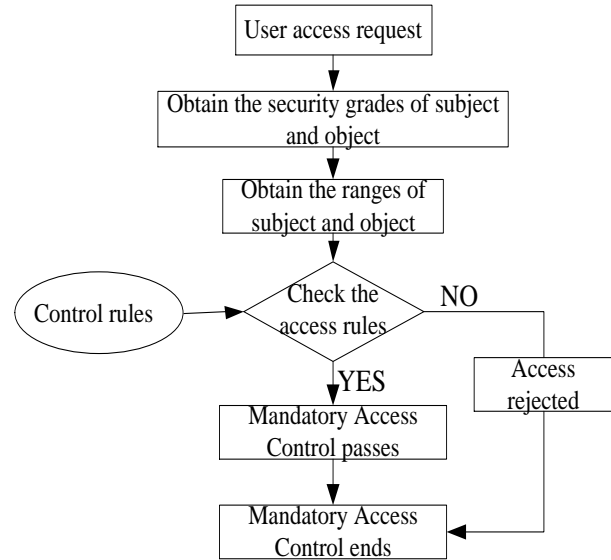Mandatory Access Control implementation flowchart is as shown in Figure2.

Figure 2. Mandatory Access Control implementation flowchart

In the flowchart, the core code of the access rule checking module is as follows:

```
#define ACCESS_DENY            0
#define READ_ONLY        1
#define WRITE_ONLY       2
#define READ_WRITE       3
enum SECRET_GRADE    // Users and object
security grade
{
      UNFURL, // unfurl
      SECRET,        // secret
      TOP_SECRET// top secret
};
enum RANGE_GRADE          // access scope
{
      NULL_, // empty
      PERSON, // person
      FILE_, // file
      PLANE // plane
};
struct OBJECT  // object property
{
      SECRET_GRADE     sec_grade;// security
grade
      RANGE_GRADE           range;  // range
grade
};
struct USER  // principal property
{
      SECRET_GRADE   read_grade; // read the
secret grade
```

```
        SECRET_GRADE  write_grade; // write the
secret grade
        RANGE_GRADE         read_range;      //
read the range
        RANGE_GRADE         write_range;     //
write the range
  };
  int Access_Control(OBJECT *D,USER *S)
  {
        if (S->read_range >= D->range) // user range
contains objective range
        {
                if   (S->write_grade   >   D-
>sec_grade)// cannot be written
                {
                        if (S->read_grade >= D-
>sec_grade)return READ_ONLY;// read only
                }
                else // can be written
                {
                        if (S->read_grade <  D-
>sec_grade)return WRITE_ONLY;// write only
                        else     return
READ_WRITE;// read and write
                }
        }
        return ACCESS_DENY;// access deny
  }
```

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 completed the access to control module. We sincerely hope that this research can provide some technical supports for the database development in the future.

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

Qu, G., Zhang, J., & Zhao, W. (2014). Primary Study on the Reformation of Production Engineering Practice Course System of the Petroleum Engineering. Journal of applied science and engineering innovation, 1(3), pp.212-216.

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