A Flexible Database Security System Using Multiple Access Control Policies*

Min-A Jeong[1], Jung-Ja Kim[1], and Yonggwan Won[2]

[1] Research Institute of Electronics and Telecommunications Technology,
Chonnam National University
300 Yongbong-Dong Buk-Gu
Kwangju, Republic of Korea
{majung,jjkim}@grace.chonnam.ac.kr
[2] Department of Computer Engineering,
Chonnam National University
300 Yongbong-Dong Buk-Gu
Kwangju, Republic of Korea
ykwon@chonnam.ac.kr

Abstract. Due to various requirements for the user access control to large databases in the hospitals and the banks, database security has been emphasized. There are many security models for database systems using wide variety of policy-based access control methods. However, they are not functionally enough to meet the requirements for the complicated and various types of access control. In this paper, we propose a database security system that can individually control user access to data groups of various sizes and is suitable for the situation where the user's access privilege to arbitrary data is changed frequently. Data group(s) in different sizes ***d*** is defined by the table name(s), attribute(s) and/or record key(s), and the access privilege is defined by security levels, roles and polices. The proposed system operates in two phases. The first phase is composed of a modified MAC(Mandatory Access Control) model and RBAC(Role-Based Access Control) model. A user can access any data that has lower or equal security levels, and that is accessible by the roles to which the user is assigned. All types of access mode are controlled in this phase. In the second phase, a modified DAC(Discretionary Access Control) model is applied to re-control the '*read*' mode by filtering out the non-accessible data from the result obtained at the first phase. For this purpose, we also defined the user group ***s*** that can be characterized by security levels, roles or any partition of users. The policies represented in the form of ***Block***(***s***, ***d, r***) were also defined and used to control access to any data or data group(s) that is not permitted in '*read*' mode. With this proposed security system, more complicated 'read' access to various data sizes for individual users can be flexibly controlled, while other access mode can be controlled as usual. An implementation example for a database system that manages specimen and clinical information is presented.

* This study was supported by a grant of the International Mobile Telecommunications 2000 R&D Project, Ministry of Information & Communication, Republic of Korea.

V. Mařík et al. (Eds.): DEXA 2003, LNCS 2736, pp. 876–885, 2003.

1 Introduction

Database security becomes more crucial as the scale of database for public and private organizations is growing and the various user access schemes are required. Recently, most relational database management systems(RDBMS) provide only some limited security techniques, which generally use a policy-based access control[1].

The most popular access control policies currently used are Mandatory Access Control(MAC), Discretionary Access Control(DAC), Role-Based Access Control(RBAC). MAC policy designates a security level to data and users, and therefore makes it possible to control the abnormal flow of information. However, the MAC policy lacks the flexibility to fulfill the conditions for a complex access control[2]. While DAC policy can control the access flexibly rather than the MAC policy, it cannot control an illegal flow of information to unauthorized users[3]. RBAC policy assigns the users to applicable roles, and the users can access to data by the access right assigned to each role. Therefore, RBAC policy can provide simple security management methods and also prevent the abused access right by allowing only least privilege to the users[4][5].

With respect to the characteristics of each access control policy above, some security models using one or two policies were proposed for the database system. Some models using the MAC policy are Access Matrix model, Task-Grant model, Action-Entity model, Wood and so on[6]. Jojodia-sandhu model and Smith-Winslett model adopt the DAC policy[7][8][9]. Sea View model is a suggestion to combine both policies[10]. Additionally, there are researches referring to the RBAC techniques that provide simple security management by Sandhu-Bhamidipati and Ferraiolo[11][12].

Those security models extend the standard relational database model, and have a drawback that a modification or alternation is not easy when security requirements are frequently changed. That is, they are not suitable to the situations when the user's access right on a data changes at any time, and also have difficulty in performing different access control for each user to the same data. For example, if two users have same access right on the same attributes but have different access right on the different tuples in a table of medical information database, it is not easy to control the individual access by the existing security models. In some situations, it is frequently required that the user who has access right on specific patient data should grant access right to some users who does not have. Consequently, a special access control is necessary for each data group of different sizes, which is formed by a combination of various tuples and attributes.

In this paper, we propose a system for user-specific access control to data groups of various sizes. The proposed system operates in two phases. The first phase is composed of a modified MAC model and RBAC model. A user can access any data that has lower or equal security levels, and that is accessible by the roles to which the user is assigned. All types of access mode are controlled in this phase. In the second phase, a modified DAC model is applied to re-control the '*read*' mode by filtering out the non-accessible data from the result obtained at the first phase. For these procedures, user groups and data groups were firstly defined and then an access rule was set up on the basis of the defined groups of user and data. The system does not extend a standard relational model but makes it possible to handle complex access control by providing different access rules to each user or user groups.