Controlling Database Security by Combination of Role-based Access Control (RBAC) and Mandatory Access Control (MAC)

Aye Aye Soe, Sabai Phyu
University of Computer Studies, Yangon
ayeayesoeucsy@gmail.com ;

Abstract

Database security is the system, processes, and procedures that protect a database from unintended activity. Unintended activity can be categorized as authenticated misuse, malicious attacks or inadvertent mistakes made by authorized individuals or processes. Database security can begin with the process of creation and publishing of appropriate security standards for the database environment. The standards may include specific controls for the various relevant database platforms; a set of best practices that cross over the platforms; and linkages of the standards to higher level polices and regulations. Proposed system presents constraint based security model implemented on student database to enhance data security by combination of Role Based Access Control (RBAC) and Mandatory Access Control (MAC).

Keywords: database security, role based access control, mandatory access control, authentication

1. Introduction

Database security is the process of creation and publishing of appropriate security standards for the database environment, including specific controls; and linkages of the standards to higher level polices and regulations. Access control models have traditionally included mandatory access control (or lattice-based access control) and discretionary access control. Subsequently, role-based access control has been introduced, along with claims that its mechanisms are general enough to simulate the traditional methods.

Role-based Access is generally recognized as being the most flexible form of access control. Traditional mandatory access control is associated with sensitive security information and incorporates the policy of one directional information flow in a lattice. This system presents database security for student database containing personal information and academic records of students and subjects.

This paper is organized as follows. Section 1 is the introduction, section 2 is related work. Database security, Role-based Access Control and Mandatory Access Control are presented in section 3. Section 4 is the proposed system design and section 5 is the system implementation and sample case study for combination of RBAC and MAC. Section 6 is the conclusion of the system.

2. Related Work

Role-based access control has received considerable attention as a promising alternative to traditional discretionary and mandatory access controls [4]. In RBAC, permissions are associated with roles, and users are made members of appropriate roles thereby acquiring the roles' permissions. This greatly simplifies management of permissions. Roles can be created for the various job functions in an organization and users then assigned roles-based on their responsibilities and qualifications. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed.

An important characteristic of RBAC is the policy neutral. RBAC is a means for articulating policy. Moreover, the access control policy can evolve incrementally over the system life cycle, and in large systems it is almost certain to do so. The ability to modify policy to meet the changing needs of an organization is an important benefit of RBAC.

Since the introduction of RBAC, researchers have discussed the relationship between RBAC and traditional models such as MAC, DAC [5] and attempted approaches on configuring RBAC to enforce MAC and DAC models. Nyanchama [4] proposes a number of access constraints that would realize the equivalent of Bell and LaPadula read-down and write-up rules. Sandhu [6] attests the flexiblity of RBAC and its ability to accommodate MAC policies by suitable configuration of role hierarchies and constraints.

This paper presents the implementation of mandatory access control in an existing role-based security system.

3. Database Security

Data protection from unauthorized accesses is becoming more and more crucial as an increasing number of organizations entrust their data to database systems. An important functionality that every database management system must follow, (DBMS) is the ability to protect data and system resources from intrusions, modifications, theft, and unauthorized disclosures. Since data in a database are related by semantic relationships, damage in a database environment does not only affect a single user or application, but the entire information system.

Database management systems must provide techniques to enable certain users or user groups to access selected portions of a database without gaining access to the rest of the database. This is particularly important when a large database is to be used by many different users within the same organization. For example, sensitive information such as student marks should be kept confidentially from most of the database system's users. A DBMS typically includes a database security and authorization subsystem that is responsible for ensuring the security of portions of a database against unauthorized access.

3.1. Role based Access Control

In RBAC, permissions are associated with roles, and users are made members of appropriate roles thereby acquiring the roles' permissions. This greatly simplifies management of permissions. Roles can be created for the various job functions in an organization and users then assigned roles based on their responsibilities and qualifications. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. To simply the RBAC, RBAC has three sets of entities called users, roles and permissions.

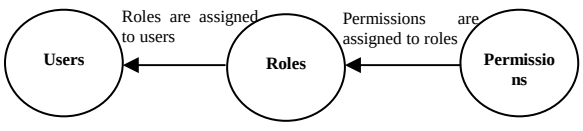

Figure 1: Implementation of RBAC

Role is a job function or job title within organization, with some associated semantics regarding the authority and responsibility conferred on a member of the role. Permission is an approval of a particular mode of access to one or more objects in the system. User can be a member of many roles as well as a role can have many users.

Main Advantage of RBAC is flexibility, proving similar levels of protection for objects in a system. Another advantage of role-based system relates to the granularity of system privilege management.

3.2. Mandatory Access Control

Mandatory access control, can be defined as "a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (e.g. clearance) of subjects to access information of such sensitivity". Clearance is the security level to which and individual user or client can access information. This clearance is usually associated with a "need to know" requirement.

Data protection for a class is determined by its label. Access to an object is determined by comparison of subject (user) level and object label.

This paper uses four security clearance values according to Security Information: The first one is Top Secret (T) which shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. The second level is Secret (S) which shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally serious damage to the national security. The next one is Confidential (C)) which shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally damage to the national security. And the final one is Unclassified (U) where there is no security restriction.

The main advantage of MAC is that it enhances the security of database. Moreover, it gives consistent view of operations

3.2.1 Classification Policy

Classification permits security level given to information. Clearance and classification determine user's clearance, a limit to access of information based on the information's classification.

Classification relation $\Rightarrow$ null < U < C < S < T

Each security level dominates itself and all others below it in this hierarchy. There are two rules defined for the mandatory access. The first one is Simple-security property, in which a subject can read an object only if the security level of the subject is

higher or equal to the security of the object (read-down). The other is *.property where a subject can write on an object only if the security level of the object is equal to the security level of the subject. (write up)

4. Proposed System

The proposed paper presents the security-related clients (subjects, users) and resources (objects) that comprise the system architecture. It implements a database security system for authentication of access data with the combination of RBAC and MAC. It includes three categories of services.

Security Policy Services define user roles (UR's), register the resources, services and methods, and grant access to roles for resources, services and/or methods. Security Policy Services also include several methods that are provided for resource servers to publish themselves, their services and methods.

Security Authorization Services are utilized to maintain profiles on the clients (e.g. users, tools, software agents, etc.) that are authorized and actively utilizing non-security services. These services allow administrator to grant users to roles.

Security Registration Services are utilized by user at start-up time for identity registration (User id and user role).

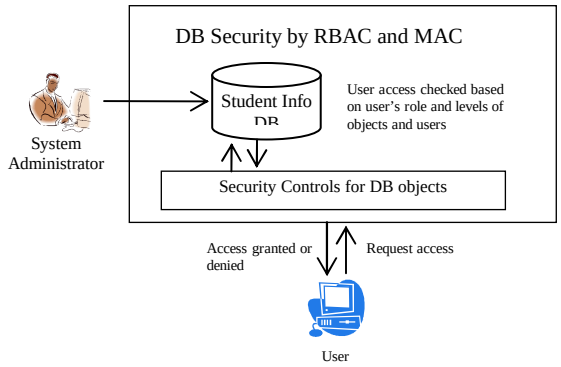

Figure 2: System overview

Figure 2 presents the overview process flow of the system. There are different roles of users to access the system. We have emphasized on student information database, storing student information. System administrator has created users, objects, permissions, roles and levels, and assigned roles to users. Users in this system may be administrators, teaching staffs such as professors, associate professors, etc., and admin staffs.

User access is granted or denied by the policies defined by combination of RBAC and MAC.

4.1. Combination of RBAC and MAC

Role-based access control eases the administration of privileges due to the flexibility with which roles can be configured and reconfigured. With roles, the principle of least privilege can be enforced where a role is assigned only sufficient functionality to realize the intended requirements. With additional rules on update and read operations, and the information they access, also requires mandatory access control. The main intention is to demonstrate that a MAC-like level of protection can be realized using role-based security.

5. System Implementation

This system is implemented using Java programming language. It is a Windows-based system and Student Information database is used for the DB security process. Process flow of the system is that user has to login before entering the system, if the login fails user has to re-enter user name and password. If login successful, this system accepts user request (Read or Write of a specific object). Based on the object, user role, permissions and levels are validated. If user has authentication to access the object, user request access is granted. Otherwise, access to requested object is denied.

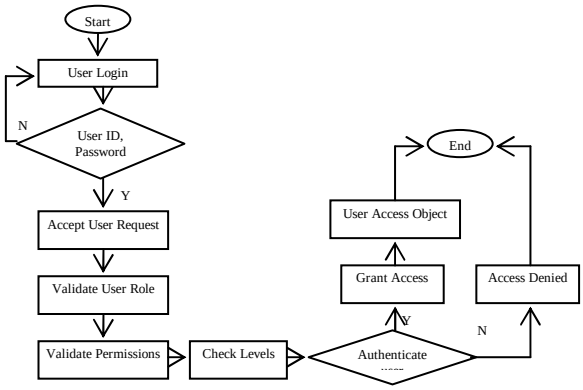

Figure 3: Process Flow of the System

Student information data includes Student's profiles (name, NRC, father's name etc.), Academic records (marks for each subjects,), Subject information and Users (school admin, teachers, staff of student affairs). Database design for student information is shown in Figure 4.

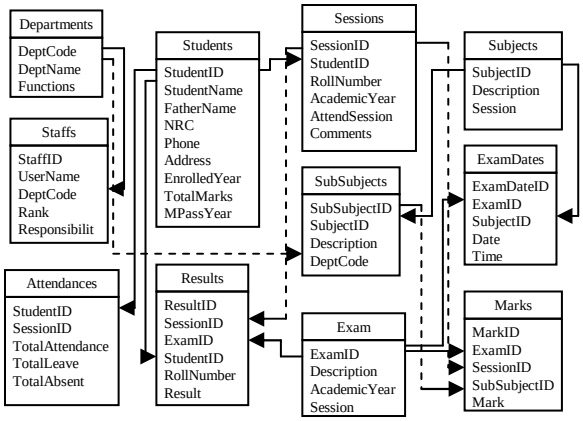

Figure 4: Database Design for Student Information

5.1. Implementation of Security Objects

In this paper security objects consist of roles, permissions and levels. Objects are data from student information database. Permissions are created upon the objects, roles has one or more permissions and roles are assigned to users. Access rights are controlled by the levels of users and accessed objects. Security object design is shown in Figure 5.

Simple Security Property: Subjects s can read object o only if $L(s) \geq L(o)$.
Strict *property: Subject s can write object o only if $L(s) = L(o)$.

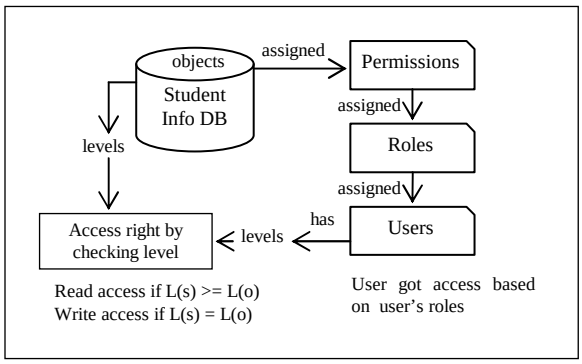

Figure 5: Security object design

5.2. Case Study

Following table shows example case study for the Database security process. In this paper, there are four classification levels for implementation of MAC, describing the levels of information sensitivity in four groups as in Table 1.

Table 1: Implementation of MAC

Level	Description	Range
T	Top Secret	30-39
S	Secret	20-29
C	Confidential	10-19
U	Unclassified	0-9

Table 2 is the objects used in this system and its levels. Table 3 shows permissions and their access right to objects. Roles and their corresponding levels are described in Table 4. Sample permissions assigned to roles are presented in Table 5.

Table 2: objects used in this system

Object Name	Level
Staffs	37
Marks	35
Students	35
Exam	25
Attendances	15
Sessions	15
Results	5
Subjects	5

Table 3: Sample Permissions

Permission ID	PermissionName	Object	Access Right
1	Read Student	Student	READ
2	Write Student	Student	WRITE
3	Read Subjects	Subjects	READ
4	Write Subjects	Subjects	WRITE
5	Read Exam	Exam	READ
6	Write Exam	Exam	WRITE
7	Read Marks	Mark	READ
8	Write Marks	Mark	WRITE

Table 4: Sample Roles

RoleID	RoleName	Level
1	Admin	39
2	Rector	39
3	Pro.Rector	38
4	Registrar	37
5	Professor	35
6	Associate Professor	33
7	Lecturer	25
8	Assistance Lecturer	22

9	Senior Tutor	15
10	Junior Tutor	5
11	Dean of School	38
12	Head of Department	35
13	Staff	5

Table 5: Sample Permissions assigned to Roles

RoleID	PermissionID
5	1
5	2
5	7
5	8
13	3
13	4

Table 6: Sample Users

UserID	UserName	Rank	RoleID	Level
P-01	Dr. Aye Aye	Professor	5	35
S-01	Daw Hla Hla	Staff	13	5

When Professor logged in, this system checked user id, password and department. If userid and password are correct, this user is allowed to use the system. The logged user, request writes access to Marks table. This system checks permissions of Role Professor has READ and WRITE access of Marks table. Level of Professor is 35 and level of Marks object is 35, therefore, Professor has WRITE access to Marks table.

6. Conclusion

This system is the implementation of secured student information database system with the combination of mandatory access control in an existing role-based security system by labeling users with clearances and all other data objects with classifications. It is based on clearances and classifications with users' roles and privileges. Therefore, combination of RBAC and MAC makes more flexible and secured organization infrastructure. By using the combination of RBAC and MAC, the system can provide confidentiality, restriction. Moreover, administrators and users of the system can effectively manage and maintain the important information resources with consistent security policies.

7. References

[1] Ferraiolo D. and Kuhn R., "Role-Based Access Control", Reprintted from 15th National Computer Security Conference, 2007.

[2] Ma J., "Implementation of Mandatory Access Control in Role-based Security System", CSE367 Final Project Report, 2001.

[3] Moffett J.D. "Specification of Management Policies and Discretionary Access Control", University of York, Department of Computer Science, June 2002.

[4] Nyanchama, M. & Osborn, S. "Modeling mandatory access control in role-based security systems", In proceedings of the IFIP Working Group 11.3 Working Conference on Database Security. Elsevier North-Holland, Inc., Amsterdam, The Netherlands, 37-56, 1996.

[5] Osborn, S., Sandhu, R., and Nunawer, Q. "Configuring Role-Based Access Control To Enforce Mandatory And Discretionary Access Control Policies", ACM Trans. Info. Syst. Security, 3, 2, 2000.

[6] Sandhu, R.S. "Role hierarchies and constraints for lattice-based access controls", In Proceedings of the Conference on Computer Security (ESORICS 96, Rome, Italy), E. Bertino, H. Kurth, G.Martella, And E. Montoliva, Eds. Springer-Verlag, New York, NY, 65-79. 1006.

[7] Wang H. and Yan L., "Implementation of Mandatory Access Control in Role-based Security System with Oracle Snapshot Skill", CSE 367 Independent Study Final Project Report, 2001.