Payroll System Using Role-Based Access Control

May Phyu Kyaw, Yuzana
Computer University (Pyay)
mayphyukyaw87@gmail.com, yuzana.yzn@gmail.com

Abstract

Security requirements approached at the enterprise level initiate the need for models that capture the organisational and distributed aspects of information usage. Such modifies have to express organization specific security policies and internal controls aiming to protect information against unauthorised access and modification, and against usage of information for unintended purposes. This system describes a systematic approach to model the security requirements from the perspective of job functions and tasks performed in an organization for the payroll system. The basis of access control policy in this system is to construct of a role. Roles are granted permissions according to the job functions that exist in an organisation, and then users are assigned to roles on basis of their specific job responsibilities. This paper intends for payroll system using Role-Based Access Control (RBAC). The central notion of role-based access control is that users do not have discretionary access control to enterprise objects.

Keywords
Secure System, Access Control, Role based Access Control

1. Introduction

In today's computing world, when people all over the world enjoy every aspect of information technology, information security has become a very urgent and complex problem. Unauthorized accesses to protected information can lead to unimaginable damages. Providing a secure, flexible, policy neutral and yet simple to administrate access control model is the ultimate aim of many security researchers and engineers.

Different access control models, which offer certain advantages, have been proposed, but a complete, well-studied model is still to be built. One of the promising approaches to solving access control tasks is the role-based access control model.

Role based access control model has attracted a great deal of attention, mainly because of its advantages over other existing access control models. National Institute of Standards and Technology (NIST) has defined a role-based access control model.

2. Related Work

In the recent study of access control requirements in organisations conducted by the National Institute of Standards and Technology (NIST), it has been found that access control decisions were based on the roles individual users take on as part of an organisation. For example, the roles an individual associated with a hospital can assume include among others doctor, nurse, and a clinician. Roles in a bank include teller, loan officer, and an accountant.

When roles are introduced at the application level to control access to the application data, they offer an excellent opportunity to realise benefits in securing organisation's information assets, similar to the benefits of employing databases instead of files as the data storage system. Roles consolidate scattered access rights into a unified service which can be better managed while providing the exibility and customisation required by individual applications.

Over the past years roles and role-based access control (RBAC) has been used in a variety of forms for computer systems security. Earlier work presented the proposals for incorporating roles into the existing security mechanisms, such as usage of mandatory controls and type enforcement [6], extensions to SQL security system and access control lists (ACLs) [1], and creation of a subset of trusted systems [5]. Introduction of roles at access control level draw attention to many security issues not covered by the traditional mechanisms and as such role-based access control has been separated into a policy-neutral alternative to classical discretionary and mandatory access controls.

Recently the definitions of basic concepts and main features involved in role-based access control were described by [2] and [4]. RBAC regulates the access of users to information and system resources on the basis of the particular function a user is allowed to perform in an organisation. Instead of specifying access rights for each individual user, access authorisations to objects, called permissions, are associated with roles. Roles are then allocated to users according to the current functionality requirements. Since the variety of roles is relatively persistent with respect to user turn-over and function re-assignment, RBAC provides a powerful mechanism for reducing the complexity, cost, and potential for error when administering access rights in a computer system. These advantages of RBAC have been extensively analysed by Gligor and Lorenz [3] and many others. Various new proposals have emerged targeting specific issues in role-based access control.

3. Secure System

Information is an asset for every organisation. The constantly increasing impact of computer systems on the functioning of organisations results in concerns about threats to the information usage. Unfortunately, some basic characteristics of computer systems, that provide overall availability of data and system services, imply risks to information. The inability of computer system to protect the confidentiality and integrity of information may cause serious financial and legal problems in an organisation. These concerns have all contributed to security, approached from an information- oriented perspective, becoming an important issue in a computer system. The primarily objectives of the security model presented in this work are expressed in terms of protecting information against the unauthorised access and modification, and against the usage of information for unintended purposes.

Any modeling of the computer system's security must be towards reaching the security goals. The main objectives of security concentrate upon protecting information from unauthorised disclosure and preventing unauthorised actions and improper modification of information. Therefore, the essence of a security model must be to ensure that system users can only gain access to those system resources, including information and programs, for which they have proper authorisations. The basis for these authorisations is mainly derived not from the ability and trust placed upon a user, but from a legitimate need to access the resources. The needs are formulated in advance by analysing and modeling requirements that originate in a realistic computing and organisational environment.

4. Access Control

Access Control mechanisms ensure every access to a system and its resources are controlled according to a set of predefined policies. It is one of the major security mechanisms used to achieve confidentiality, integrity and availability in software systems. Confidentiality means information must be kept private, only authorized users can read the information. Integrity means information must be protected from being altered; only authorized users can write the information. Availability means information must be available for use. Access control technologies are:

-User-based Access Control
-Role-based Access Control
-Policy-based Access Control
-Content Dependent Access Control
-Context-based Access Control
-View-based Access Control
-Mandatory and Discretionary Access Control

Access control is the traditional center of gravity of computer security. Its function is to control which principals such as persons, processes, machines have access to which resources in the system which files they can read, which programs they can execute, how they share data with other principals and so on. Access control assumes the existence of an authentication process.

5. Role Based Access Control

In computer system security, Role Based Access Control (RBAC) is an approach to restrict system access for authorized users. Role Based Access Control (RBAC) is popular because it purports to advance permissions configurations towards the common goals. RBAC entails mapping the different “roles” (a “role” is a user group with access to a specific group of resources) in an organizational hierarchy and defining a profile of access permissions to the network’s resources for each role. Then each user is assigned one or more roles, providing him/her with the access permissions defined by those roles. A user with super-user access may be classified in every role, whereas someone with less need-to know may be classified in only one or two roles. RBAC has the potential for refining granularity by assigning specific types of privileges to specific resources. Users in a certain “role” may be granted access to “read” but not to “write” certain files.

6. Motivation of Role Based Access Control

The initial motivation for developing RBAC models was to improve the security management in the commercial sector. RBAC is either directly implemented or supported in some form in several commercially available products. More than any other commercial application software, DBMSs (database management systems) provide access control at several levels of granularity including provision for content dependent or workflow based controls. Since an application system developed using a DBMS can contain a large amount of data with highly differentiated access permissions for different users depending upon their function or role within the organization, database management can perfectly make a good use of RBAC mechanism for management of authorizations or privileges.

The principal motivation of RBAC is to simplify administration. In large organizations the number of roles can be in the hundreds or thousands, and users can be in the tens or hundreds of thousands, maybe even millions. To be effective, management and administration of RBAC in such systems need some form of decentralization and automation without loosing central control over broad policy. An appealing possibility is to use RBAC to manage itself.

7. Benefits of RBAC

A properly administratored RBAC system enables users to carry out a broad range of authorized operations, and provides great flexibility and breadth of application. Using roles to determine and manage access permissions allows system administrators to better incorporate least privilege and separation of duties into administrative policies.

Key benefits of RBAC are:

-Simplified systems administration

-Enhanced organizational productivity

-Reduction in new employee downtime

-Enhanced systems security and integrity and

-Simplified regulatory compliance

8. Components of Role Based Access Control

When designing an access control model, the first issues that must be addressed are the definitions of subjects and objects, and the types of access provided by the system which described as permission. When the user has the permission on the transaction, the administrator can be granted the authority of access transaction to the user.

8.1. Subjects and Objects

There are two types of subjects: the users of the system and the transactions that execute on behalf of those users. Users can access objects only by executing transactions on these objects. A transaction here refers to the transformation procedure (a program, or a set of executable operations), which upon invocation manipulates data items or causes consumption of a system resource.

The behaviour of the transaction and the type of data it can operate on are determined at design time. A transaction embodies different methods and granularity than simple access modes do, as can be seen in the following example. Tellers in a bank are able to execute a savings deposit transaction, requiring read and write access modes to the specific fields within a savings file. An account supervisor is allowed to perform correction transactions, requiring the same read and write access modes to the same file as the teller's. The difference between these two transactions is in the whole process executed and in the values written to the transaction log file.

8.2. Permissions

The system protection in an access control model is realized in terms of permissions. It is generally accepted that permission describes an approval of a particular access right to an object or set of objects.

In presenting the RBAC model we are concerned with protecting computer system resources and data from unauthorised access and modification by users of this system.

Since we have accepted that the only access rights the users have is to perform transactions, permission in this work is viewed as the right to execute a particular transaction on a specific object from the defined set of objects. In payroll system, there are three roles: administrator, manager and staff. The following figures consist of which user and which permission get.

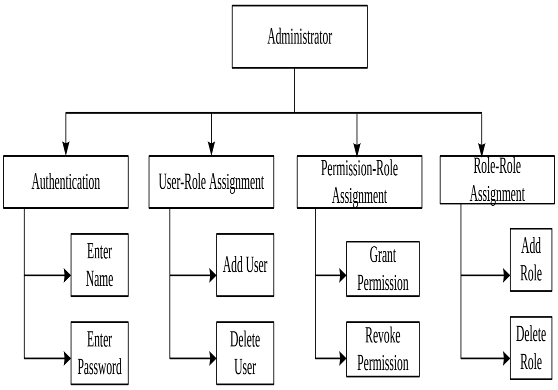

Figure 1. Structure chart for administrator

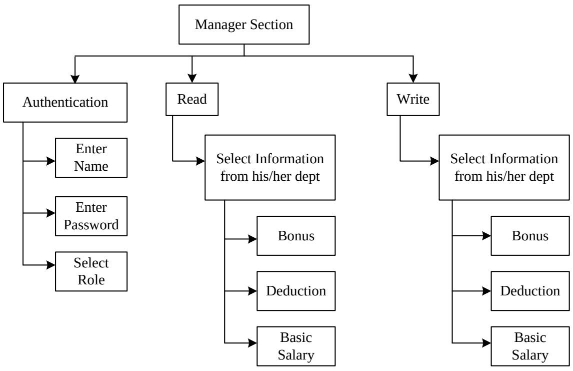

Figure 2. Structure chart for manager

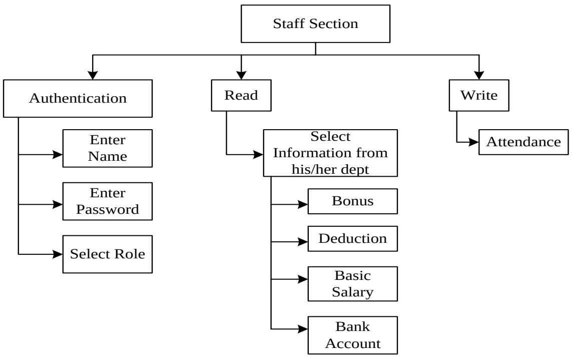

Figure 3. Structure chart for staff

8.3. Role Hierarchy for Payroll System

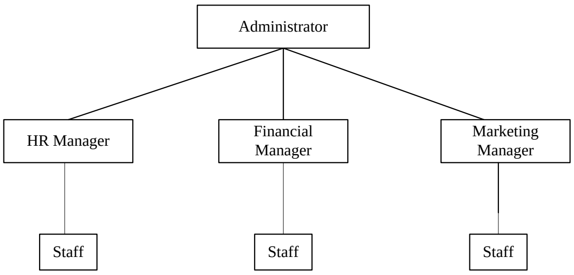

Figure 4. Role hierarchy for payroll system

Role hierarchies are natural way of organizing roles to reflect authority, responsibility, and competency. When operations overlap, hierarchies of roles can be established. Role hierarchies support the concept of multiple inheritances, which provides the ability to inherit permission from two or more role sources and to inherit user membership from two or more role sources.

Under the RBAC framework, users are granted membership into roles based on their competencies and responsibilities in the organization. When a user is associated with a role, the user can be given no more privilege than is necessary to perform the job. Roles can have overlapping responsibilities and privileges; that is, users belonging to different roles may need to perform common operations. A role hierarchy defines roles that have unique attributes and that may contain other roles; that is associated with another role. In payroll system, there are three departments such as Human Resource (HR) Department, Financial Department and Marketing Department. Each department has manager. And staff from each department has little permission than manager.

8.4. User-Role Authorisations

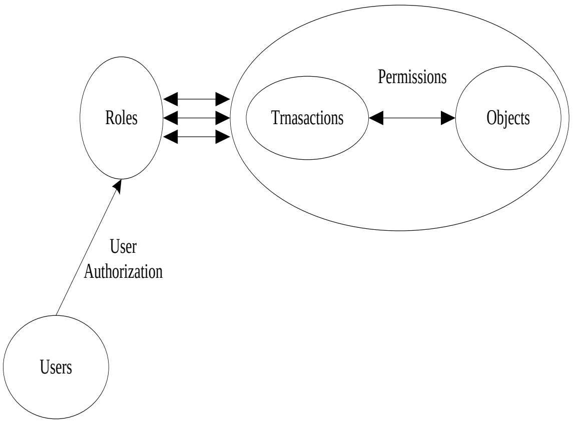

Figure 5. User-role permission mapping

The permissions associated with a role are administered as a single unit such that authorisation to access a role puts all the role's permissions at the disposal of an authorised user and thus confers access rights grouped in the role to the user. A role acts as a gateway to system permissions and accessible information, illustrated in the following figure. Associated with each role is a user authorisation list. This list identifies the users who are authorised to access the role.

9. Architecture of the System

This security model provides with its security constraints and role-based authorizations in payroll systems. Access control mechanisms in the RBAC model require that security attributes are kept about users, roles, transactions, objects and tasks.

The system administrator creates the role hierarchy and assigns a set of permissions for each role based on the security policy; in our case, the payroll system security policy. The permission-role assignment supports permission inheritance, which is dictated by role hierarchy.

First a user presents his username and password to the system server to be authenticated. After a successful authentication the user has the option of choosing one of his assigned roles to be the active role for his current session. The system management then sends an authorization request to role server to retrieve role information. The authorization certificate is then sent back from role server to system management, which in turn checks the authorization status based on its permission-role assignment information. After a successful authorization, the user can execute transactions in the server based on the user's role instead of his identity. The access control process proceeds as the following.

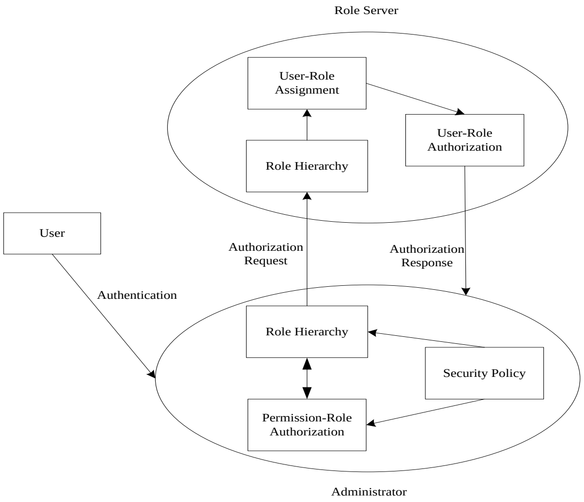

Figure 6. System architecture

10. Process Flow of the System

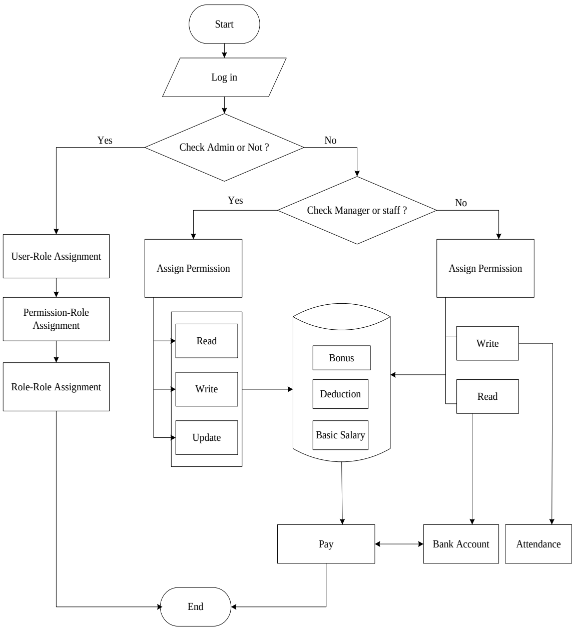

Figure 7. Process flow of the system

Firstly, the users must log in to determine their roles. If the user is administrator, he has the permissions of the administrator role. The administrator has permission of

- User-Role Assignment

-AddUser

-DeleteUser

-Permission-Role Assignment

-GrantPermission

-RevokePermission

-Role-Role Assignment

-AddRole

-DeleteRole

If the user is not administrator, there needs to determine another roles. If the user is manager, he has the permissions of manager role. They are read and write the objects in database from their departments. The manager calculates the salary for staff based on their attendance, leave and over time in order to pay bonus and deduction. When manager pay the salary to staff, this amount will enter into Bank Account. If the user is staff, the staff can read their objects and bank account in database and write only attendance.

11. Security Attributes

User security attributes describe what roles are authorised to the user. Role security attributes consist of permissions associated with the role, users authorised for the role, and names of roles that are strongly/weakly exclusive with the role. A role hierarchy describing inheritance relationships between roles may exist as a separate structure.

Types of objects that a transaction can operate on, and the names of tasks in which it can be used are referred to transaction security attributes. Object security attributes define the permissions required to operate on the object. Task security attributes are represented as task authorisation templates, describing permissions that are enabled for each task's instance together with the names of roles to which permissions belong. A defined critical combination of transactions within the task is also a security attribute of the task.

A role manager has to accomplish the following tasks:

-verify that roles are correctly defined;

-ensure consistency in role hierarchy;

-monitor user authorisations to roles.

First task is concerned with the application of constraints that directly deal with permissions given to roles. In addition to ensuring that each role has minimum number of permissions required, the role manager must verify that no role violates an enforced separation of duty policy. Second task ensures consistency of role relationships in role hierarchy.

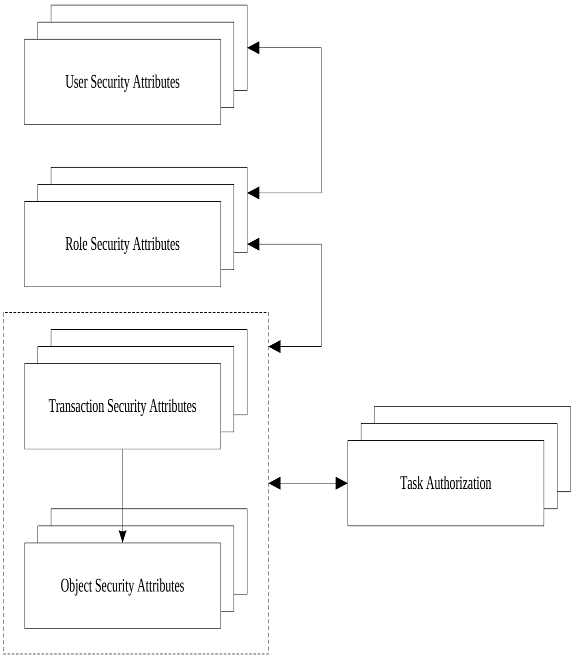

Figure 8. Security attributes

12. Conclusion

This paper provides a security model for access control and authorisation management that allows permission to control the payroll system by using RBAC. The common characteristic of traditional access control approaches is that they operate using simple access modes such as read, write, execute, that control access at the operating system level. At the application level, however, one would like to see access rights which relate to richer and more complex operations.

This system will has several advantages. One advantage is that applications need not change when access conditions for roles are changed. Applications use the methods of the application interface class whose methods have the same names, types, and parameters as the methods in the basic access methods class. The methods of the application interface class and the methods of the basic access methods class are fixed and remain constant over time. Another advantage of this approach is that access conditions for roles are easily changed. Access conditions for roles are located exclusively within the role classes. Consequently, role policy changes do not require modifications to the applications themselves.

13. References

[1] Barkley, J. Workflow management employing role-based access control U.S. Patent #6,088,679, NIST, July 2000, http://www.uspto.gov/patft

[2] Ferraiolo, F. D., Sandhu, R., Gavrila, S., Kuhn, R. and Chandramouli, R.A proposed standard for role-based access control, 2000, http://csrc.nist.gov/rbac/

[3] Gligor, D. V., Gavrila, I. S. and Ferraiolo, F. D. On the formal definition of separation-of-duty policies and their composition. Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 172-183, Oakland, CA, May 1998.

[4] Sandhu, R., Ferraiolo, D. and Kuhn, R. The NIST model for role-based access control: towards a unified standard**,** Proceedings of the Fifth ACM Workshop on RBAC, pp. 47-63, July 2000.

[5] Steimuller, B. and Safarik, J. Extending role-based access control model with states. Proceedings of the International Conference on Trends in Communications (EUROCON'2001), Vol. 2, pp. 398 399,2001.http://www.ieeexplore.ieee.org/iel5/7466/20308/00938147.pdf

[6] Thomsen, D., O'Brien, D. and Bogle, J. Role based access control framework for network enterprises. Proceedings of the 14th Annual Computer Security Applications Conference, pp. 50-58, 1998, http://www.ieeexplore.ieee.org/iel4/5961/15949/00738571.pdf.

[7] A role and context based security Model Yolanta Beresnevichiene January 2003 15 JJ Thomson Avenue Cambridge CB3 0FD United Kingdom phone +44 1223 763500 http://www.cl.cam.ac.uk/

[8] A Proposed Standard for Role-Based Access Control David F. Ferraiolo National Institute of Standards and Technology , Ravi Sandhu George Mason University, Serban Gavrila VDG Incorporated D. Richard Kuhn and Ramaswamy Chandramouli National Institute of Standards and Technology

[8] Malaysian Journal of Computer Science, vol 14, No.2

December 2001, pp 20-25, RBAC in Kidney Dialysis Information Sysem. boonpeng@hotmail.com, omar@fsktm.um.edu.my, mustaffa@fsktm.um.edu.my