USER ACCESS CONTROL AND SECURITY MODEL

Cahyo Crysdian, Harihodin b. Selamat, Mohd. Noor b. Md. Sap
(crysdian@yahoo.com, harihodn@itp.utm.my, mohdnoor@fsksm.utm.my)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia
Jalan Semarak 54100 Kuala Lumpur Malaysia
Telp: 603-2904957, Fax: 603-2918059

Abstract: *Securing information system becomes the highlight of technology following quick development of computer networking and the Internet. People have known the method to enforce security over a database, but the necessities to get more secure system never reach boundaries. Now days the trend of information system is the open connection system where users are able to access system from many places. It leads the involvement of user access control as a part of database security since it takes a big role in governing access request of each user. This security component serves as a part of defense to secure data contained in the system. Development of user access control began on the early of seventies with DAC technology. Right now technology of user access control has reached sophisticated method with RBAC, but development of organization using information system and the development of information system itself push the improvement of user access control technology. This paper provides information about security system with the emphasis on user access control, which includes DAC, MAC and RBAC and the implementation of each user access control in security model. Comparison of each user access control method is given at the end of the paper.*

Keyword: Database Security, Security, User Access Control, Access Control

1. Introduction

In the recent development of computer and networking database security is facing a big challenges to protect information contained in the information system. There are a lot of possible event leads to security breach over a database, and therefore causing security violations. Security violation is the condition when the security mechanism fails to protect information contained in the system. (Krause et. al, 1997) classified security violations into three categories:

a. Improper release of information, which has the relevancy with the reading process done by the unauthorized user.
b. Improper modification of data, which includes information mishandling and modification by unauthorized user.
c. Denial of service, which prevents user from using system resources or accessing data.

Potential events causing security violation can be defined as a threat. (Khelalfa, 1997) classified the threat as accidental and intentional. The examples of accidental threat are natural disasters, human errors and the errors in the hardware and software of computer. On the other hand, the intentional threat can be called as an attack as it is done intentionally by somebody or an organization to offence an information system that brings the dangerous condition to that system. The examples of this threat are a hostile agent that modifies the data of the database improperly and the user who abuse his privileges.

There are three aspects that must be considered in conducting security over a database. These aspects are secrecy, integrity and availability. Secrecy iş the protection from improper information disclosure. This protection prevents unauthorized user getting the information by direct retrieval or logical inference .(indirect retrieval). Integrity is the protection from improper modification of information. The forbidden cvents are "append" and "write" access to database by unauthorized user, insertion of false data and destruction of data. Availability is related with the availability of system resources and information, it means the information and system resources must always be available when the authorized user access them, and the system must not deny the operation or service run by the authorized user.

The mechanisms to gain those security aspects are discussed in this paper with the emphasis on user access control and its implementation in the security model. The explanation of user access control technology that comprises DAC, MAC and RBAC will be given in the later section, whereas the capability of each method to cater organization requirement that consist of business and military environment will be discussed in the separate chapter. The remaining of this paper is organized as the following:

Section 2 gives a brief explanation about each mechanism that is possible to be done in conducting security. Section 3 explains more about user access control method that consist of DAC, MAC and RBAC and how they work. Section 4 explains about security model to implement each user access control method. Section 5 gives a discussion on each access control technique by comparing each other, and the involvement of user access control in the organization will also be explained in this section. Conclusion of this paper containing proposed future research direction is given in section 6.

2. Security Control

Security control is the effort to perform security over a database using a certain mechanism. (Denning, 1983) classified security control into:

a. Flow control
b. Inference control
c. Cryptographic control
d. Access control

Flow control governs information flowing from one security level to another security level (Sandhu, 1993). It prevents the flowing of information contained in an object into the less protected object. The information flowing can be happened explicitly, e.g. through a copy, or implicitly, e.g. through a hidden program such as Trojan horse and virus (Castano et. al, 1994; McLean, 1990). This control permits the flowing of information only if one of the two following condition satisfied, i.e. the source object and the destination object have the same protection level or the source object has the lower protection level than the destination object.

Inference control prevents the information disclosure done by unauthorized user who uses many ways of deduction (Khelalfa, 1997). The focus of this mechanism is to deter indirect detection to the information. Cryptographic control prevents the information to be understood by the unauthorized user (Menezes et. al, 1996). This mechanism converts the information into a different form of information using a certain way. Only the authorized users are able to understand the meaning of information.

Access control manages and regulates the direct access to the information system. This mechanism performs security control based on the security policies supplied to the system. As it has the function to regulate the access request of each user, it deals with individual user registered in the system. In the system implementation, access control mechanism is enforced in the security model (McLean, 1994). Further description on the security model will be given in section 4. From this point, paper will focus more on the user access control and its mechanism.

3. Access Control

Access control is the mechanism to obtain security control over the database by governing the direct access to the information system based on the access policies supplied to the system (Sandhu and Samarati, 1994). Access control must ensure that every access to the system is occurred exclusively (Castano et. al, 1994). The access control system comprises the following components:

a. Subject is the active entities accessing system resources. Subject can be a user or a process, and the system must be protected from this component.
b. Object is the passive entities that must be protected from getting the access by unauthorized subject. Object can be considered as the system resource.

Access control can be classified into the following categories:

1. Discretionary Access Control (DAC)
2. Mandatory Access Control (MAC)
3. Role Based Access Control (RBAC)

The explanation of those methods will be given in section 3.1, 3.2 and 3.3 respectively.

3.1. Discretionary Access Control (DAC)

The DAC governs the access of the subject to the object based on the user's identity and authorization rules applied to the system (Pernul, 1995; Baraani-Dastjerdi et. al, 1996). User's identity and authorization rules are used to specify the access rights owned by the user such as read, write, execute, open, close, etc. The architecture of DAC can be shown in the figure 1.

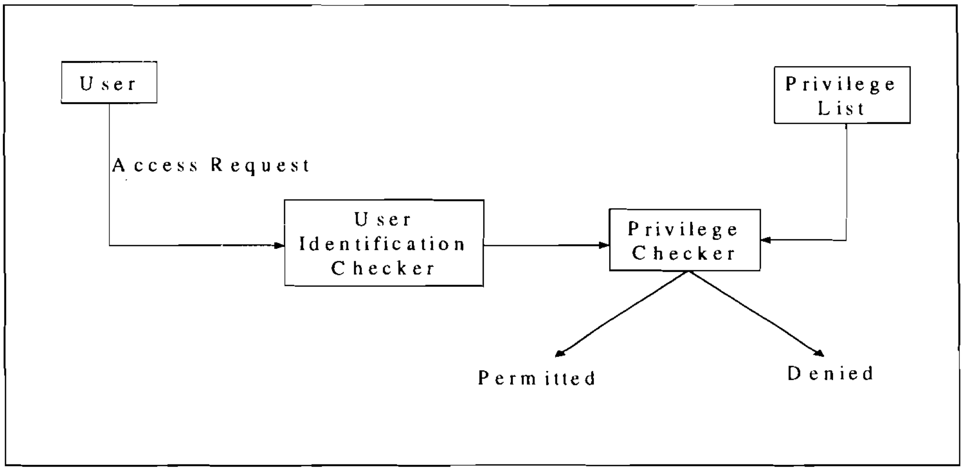


Figure 1. DAC architecture

Every access request to the information system is passed through the user identification checker to define who made the request. After the user could be identified, the privileges checker compare the access request with the privilege list, which consist of the privileges belongs to each user. In here the decision whether the access is denied or permitted is made. The other characteristic of DAC is the condition that the users are permitted to have the privilege to propagate the access right of the object belongs to them to the other user (Pernul, 1995; McLean, 1990).

Due to its simplicity, DAC has been adopted in various systems such as UNIX, AS/400 and Windows NT. In those systems, user is allowed to have its owñ files and to grant the permission of accessing those files to other users. Thus, user becomes the administrator of its own data.

3.2. Mandatory Access Control (MAC)

The MAC governs the access of the subject to the object in the system based on the classification level owned by subject and object (McLean, 1990; Pernul, 1995; Baraani-Dastjerdi, 1996). This access control applies the tight mechanism and introduces multilevel data to manage and regulate the access request. Every subject and every object are assigned the security level based on how important the subject and how secret the object in the system (McLean, 1990; Sandhu and Samarati, 1994). The architecture of the MAC is depicted in the figure 2.

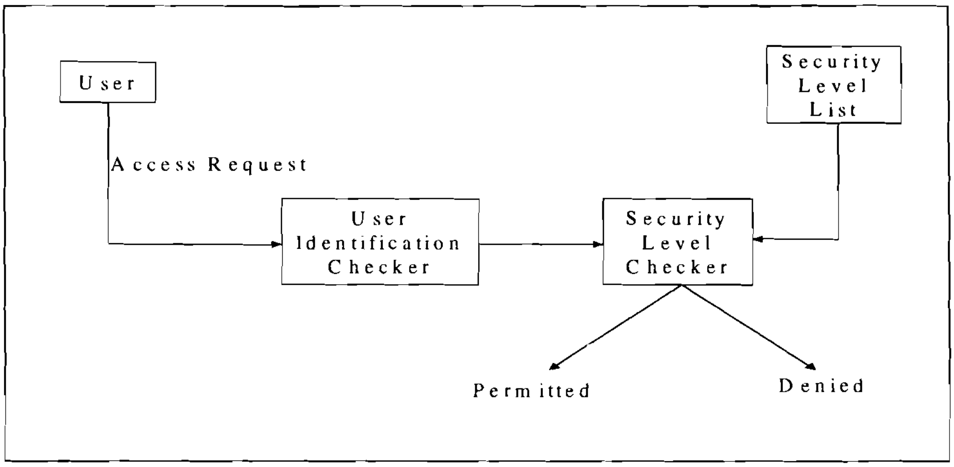


Figure 2. MAC architecture

Every access request is passed through user identity checker to recognize the user who makes the request. After the identification of user is known, then security level checker compares the security level of object being accessed and the security level of subject made an access based on the security level list. The output of security checker is the decision to permit or deny the access request.

Like the one proposed by Bell-LaPadula, security level can be classified into TS (top secret), S (secret), C (confidential) and U (unclassified) which the TS > S > C > U. Subject is permitted to access an object if security level of subject is greater or equal than the security level of object. If an object owns security level S, a subject that is allowed to access this object must have security level TS or S.

Not many systems adopted this method. Assigning security level to every user and object in the system is not an easy task, especially for the big system that contains many users and data (Sandhu and Samarati, 1994). An example of the system that adopted this method is Sea View model (Castano et. al, 1994).

3.3. Role Based Access Control (RBAC)

RBAC controls the access request of a subject to an object based on the roles that is supplied to the system. A role is the functions or transactions in which a user is permitted to perform within an organization (Ferraiolo and Kuhn, 1992). A role can belong to an individual user or a group of users. The information contained in the role includes the separation of duties, responsibilities and qualifications of the user (Baraani-Dastjerdi et. al, 1996). The roles must be maintained and updated to follow any modification within the organization. Therefore if there are any modification in the organization such as a new user is added to the system, some users resign from the organization or some users are moved from one department to another, the system is still able to control access request to the database. Role maintenance and updating are the responsibilities of system administrator. The architecture of RBAC is depicted in figure 3.

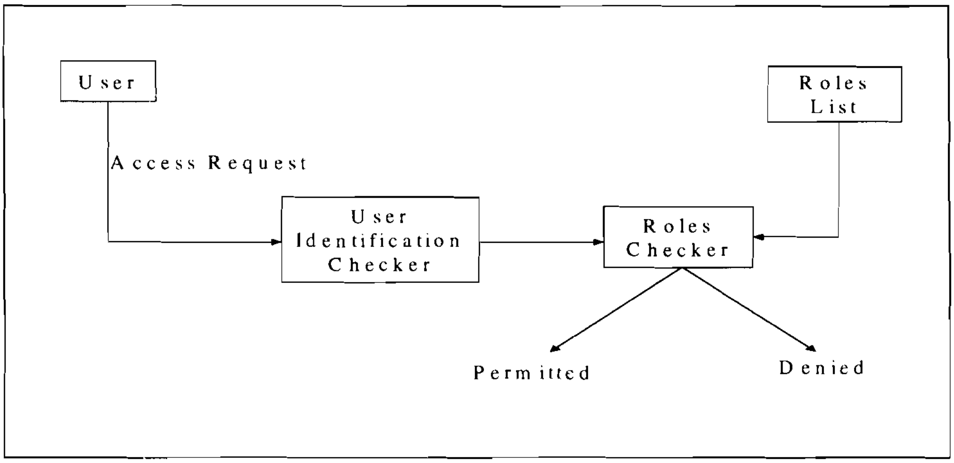


Figure 3. RBAC architecture

Every access request is passed through the user checker to recognize who issued the request. After the user made. the request is known, then the request is compared with the roles owned by the user to specify whether the request is permitted or denied. If the request satisfies the roles belong to the user, request will be permitted, otherwise it is denied.

(Ferraiolo and Kuhn, 1992) specified the differences between RBAC and DAC as the followings:

a. RBAC governs the access request based on the function of each user as a part of the organization, whereas DAC governs the access request based on the ownership of each object.
b. DAC allows users to pass their privilege to the others, whereas RBAC does not allow this operation since the objects are owned by the organization and the users just follow their function in the organization.

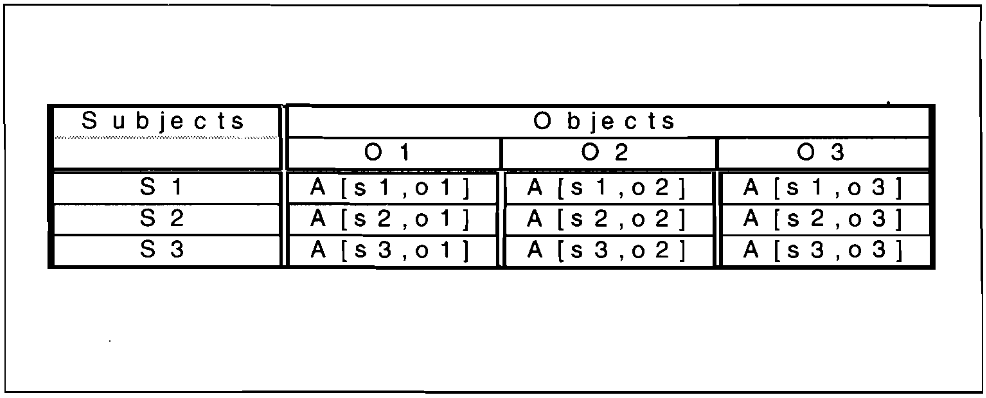
4. Security Model

As stated in section 2, security model is the mechanism to enforce access control method. The objective of security modeling is to produce a conceptual model based on the requirement that describe the protection need by the system (McLean, 1994). Since security model deals with conceptual model, it must be freed from any constraint of the implementation such as software constraint, operating system constraint, hardware constraint, etc (Castano et. al, 1994).

With respect to user access control, security model can be categorized into three groups, i.e., discretionary security model, mandatory security model and role based security model. The same with access control system, security model also applied the same definition of subject and object. Subject is the active entities that access the object and object is the passive entities that must be protected.

4.1. Discretionary Security Model

As stated in its name, this model aims to enforce DAC (Pernul, 1995), therefore the bases of this model are the users identity and the authorization rules supplied to the system. In this area, several models were proposed to formalize security mechanism under DAC. The first model appeared was access matrix model that was proposed by Lamson (1971) and extended by Graham and Denning (1972) and finally formalized by Harrison, Ullman and Ruzzo (1976). To represent security mechanism, this model uses a matrix. The matrix correlates subject, object and the authorization owned by subject to each object. If S is a set of subjects (active entities), O is a set of objects (passive entities) and A is the authorization of subject to object, then the access matrix model can be shown in figure 4.



Subjects	Objects		
	O 1	O 2	O 3
S 1	A [s 1 ,o 1]	A [s 1 ,o 2]	A [s 1 ,o 3]
S 2	A [s 2 ,o 1]	A [s 2 ,o 2]	A [s 2 ,o 3]
S 3	A [s 3 ,o 1]	A [s 3 ,o 2]	A [s 3 ,o 3]

Figure 4. Access matrix model

As shown in figure 4, each row in the matrix represents a subject and each column represents an object. The authorization owned by each subject to each object represented by A[s,o] is the entity correlating a subject to an object. This entity denotes what subject can do to an object. Take an example on the relation of subject S1 and object O1. The possible access can be taken by subject S1 to object O1 is represented using A[S1,O1] in which it can comprises the predefined operation of subject to object such as read, write, grant, modify, etc.

The other model in this area is Take-Grant model that was proposed by Jones (1976). This model is an extension of access matrix model, to represent the authorization this model uses a graph structure instead of a matrix. Figure 5 shows the mechanism applied in this model.

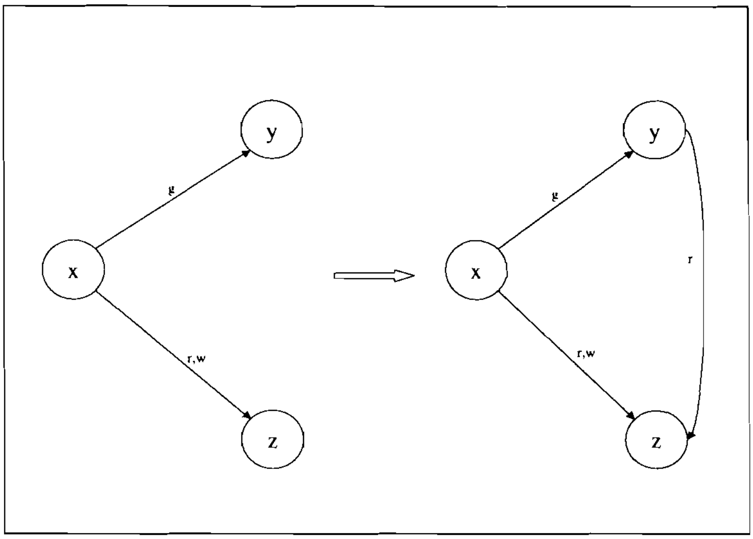


Figure 5. Take-Grant model

Figure 5 shows the step taken to grant the read access to object z. The grantor is x that has the grant access to object y and has the read and write access to object z, therefore x is capable to pass the read access to object z to subject y. In doing that operation, x takes his access right (in this case is the read operation) and sends it to y. After that, y instantly is able to access z using read operation, but y is still not able to write z before x or another user grant write operation to it.

4.2. Mandatory Security Model

This model aims to enforce MAC (Pernul, 1995). The base of this model is the security classification of subject and object. Since this model deals with the multilevel data, it is called multilevel security. The two well-known and fully established models in this area are Bell-LaPadula and Biba models. Bell-LaPadula model was proposed by Bell and LaPadula (1973, 1974a, 1974b, 1975). To perform security mechanism, this model classifies security class to subject and object in the system, i.e., top secret (TS), secret (S), confidential (C) and Unclassified (U) which TS > S > C > U. Security classes is depicted in figure 6.

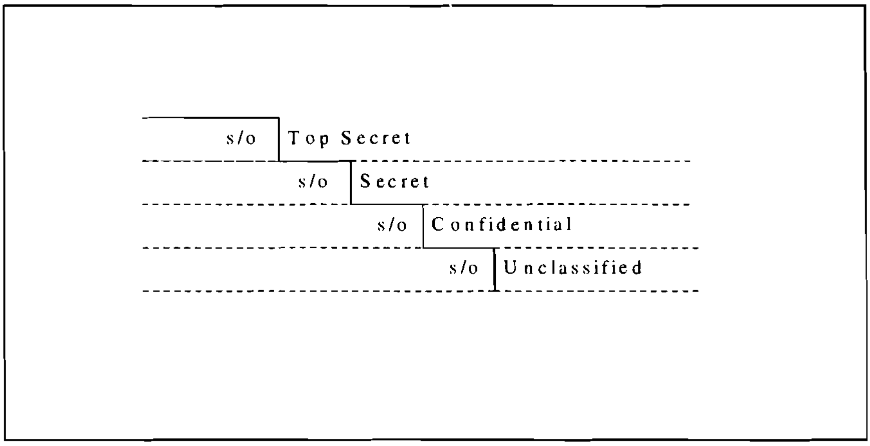


Figure 6. Security classes in Bell-LaPadula model

Bell-LaPadula model imposes two axioms in handling multilevel data:

a. The simple security property

A subject cannot have the read access to an object which security class is higher than the security class of the subject (no read up).

b. The *-property

A subject has the write access to an object which security class is higher than or equal to the security class of the subject. It has the read access to an object which security class is lower than or equal to the security class of the subject. It has the read and the write access to the object which security class is equal to the security class of subject. If f(s) is the security level of subject and f(o) is the security level of object, then each access right can be represented as the following:

Write: $f(s) \leq f(o)$
Read: $f(s) \geq f(o)$
Read/Write: $f(s) = f(o)$

These axioms are shown in figure 7. With these axioms, this model aims to prevent unauthorized release of information by achieving information secrecy.

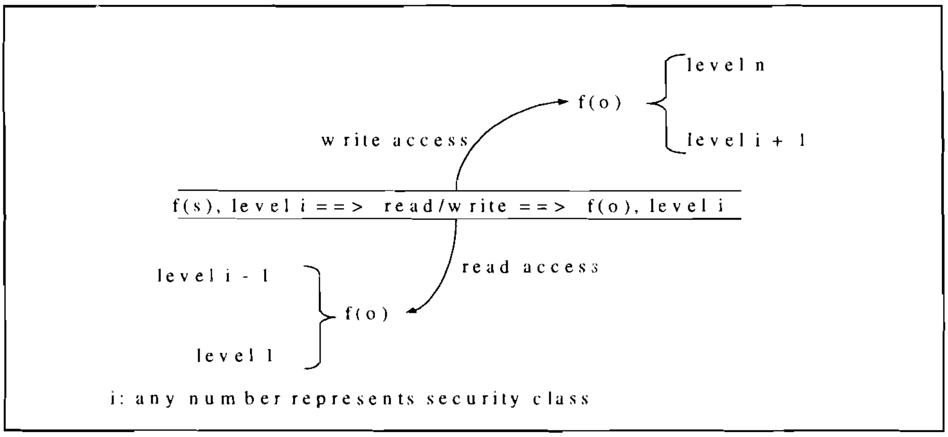

level n
f(o)
write access
level i + 1
f(s), level i ==> read/write ==> f(o), level i
level i - 1
read access
f(o)
level 1
i: any number represents security class

Figure 7. Axioms of Bell-LaPadula model

Biba model was proposed by Biba (1977) applies similar principles like Bell-LaPadula for protecting information integrity instead of secrecy. The security classes in this model are crucial (C), very important (VI), important (I) and unclassified (U) which C > VI > I > U. Unlike Bell-LaPadúla model which applies "no read up" operation, Biba model applies "no write up" operation. A subject cannot have a write access to an object which security class is higher than the security class of that subject (no write up). A subject cannot have the read access to an object which security class is lower than the security class of that subject (no read down). With these axioms this model aims to protect the system from unauthorized modification of information by achieving information integrity.

The sea view model proposed by Denning (1987) combines both MAC and DAC. This model relies on two layers, i.e., MAC model and TCB (Trusted Computing Base) model. MAC model performs MAC and classifies an access class that has a secrecy component (secrecy class) and an integrity component (integrity class). The secrecy class in the model corresponds to the secrecy of Bell-LaPadula model, whereas the integrity class corresponds to the integrity class of Biba model.

TCB model performs DAC and defines multilevel relations that are resulted from the classification of data in MAC model. The information in the TCB model is stored on the object that is mediated by MAC model (Castano et. al, 1994). The components of the Sea View model can be shown in figure 8.

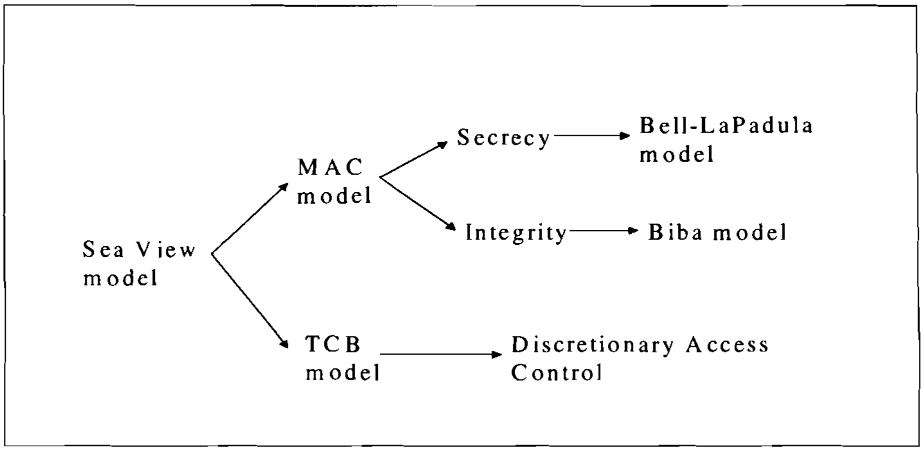


Figure 8. The components of Sea View model

4.3. Role Based Security Model

This model aims to perform RBAC. (Sandhu et. al, 1996) defined a family of four conceptual models that is known as RBAC96. This model comprises RBACO, RBAC1, RBAC2 and RBAC3. RBACO is the base model that specifies minimum requirement for the system that fully supports RBAC. The elements contained in RBACO are users, roles, permissions and sessions. Those components are the basis of Role-Based security model. RBAC1 and RBAC2 are based on the RBACO and add an independent feature to the model. The independent feature of RBAC1 is the role hierarchies, which corresponds to the permission inheritance from the other roles. And the independent feature of RBAC2 is the constraint, which corresponds to the restriction of roles. RBAC3 consolidates all of those models, i.e., RBACO, RBAC1 and RBAC2. The complete architecture of RBAC96 is depicted in figure 9.

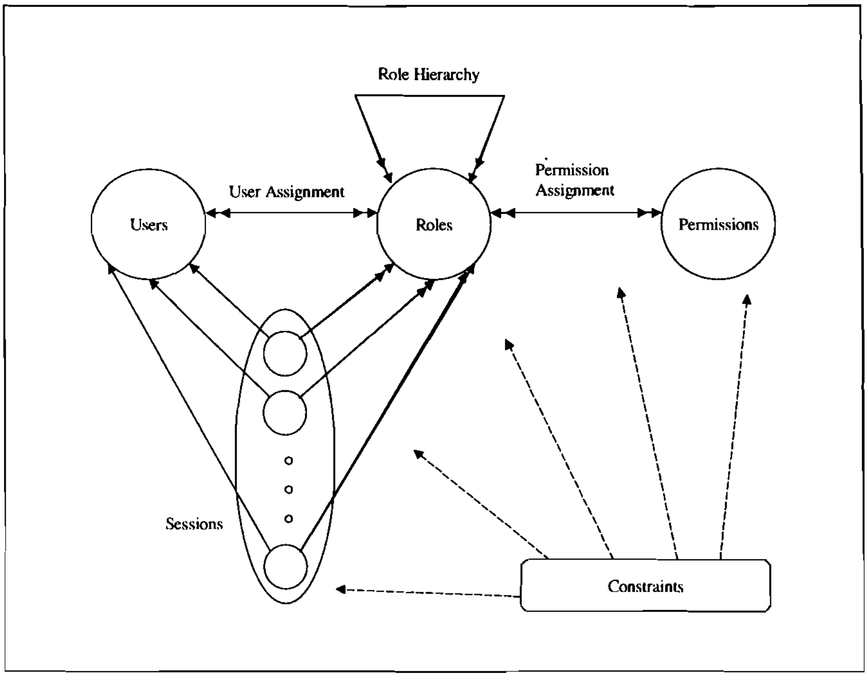


Figure 9. The complete architecture of Role Base Security model.

As stated earlier in this section the basics components constructing the model are user, role, permission and session. These components build the base model (RBAC0) and denoted by U, R, P and S respectively. User is the active entities use the system resources, usually user is a human being. Role is a job function that is done by users within the organization as explained in section 1.2.3. Permission is the access right to one or more objects in the system.

The relations that appeared in the system are user assignment and permission assignment. User assignment connects users and roles. This relation can be defined as many to many relations and represented by:

$$UA \subseteq U \times R \text{ ——————————— } (1)$$

as a user can have many roles and a role can belong to many users. Permission assignment connects roles and permissions and it is also many to many relations and represented by:

$$PA \subseteq P \times R \text{ ——————————— } (2)$$

as a role can contain some permission and permission can be used by many roles. In this model, users do not directly get the permission to access objects, the permission will be derived through a role. With this method, access request can be controlled and arranged based on the function of the user within the organization. . The session is directly established during the user active in the system. Each session is associated with a single user, and considers that a single user can have many roles. The representations of this component are:

$S \rightarrow U$: a function mapping each session to the single user ——————— (3)
$S \rightarrow 2^R$: a function mapping each session to a set of roles ——————— (4)

The other component appeared in this model are role hierarchies and constraint. Role hierarchies are used to structure the roles based on the organization structure. As stated earlier this component is used in RBAC1 and RBAC3. Role hierarchies consider the authorization and the responsibilities of the users within the organization. The example of role hierarchies is depicted in figure 10, which represents the relation of roles contained in Accounting department.

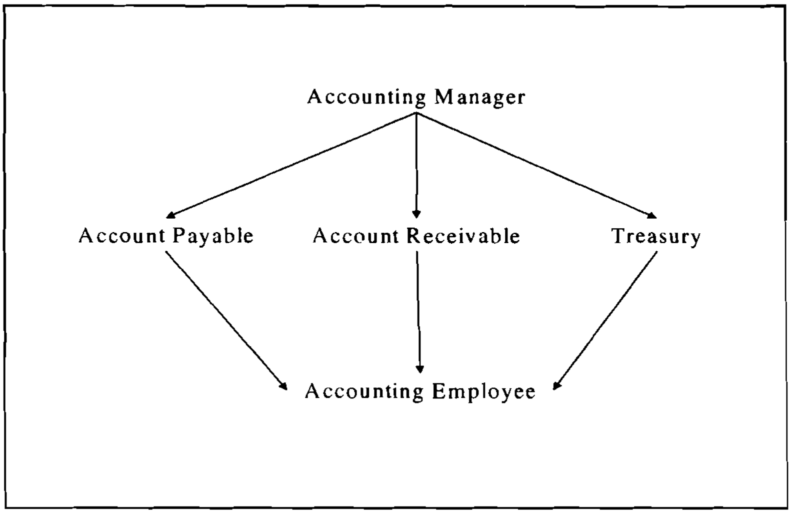


Figure 10. Role hierarchies

Constraint is used in RBAC2 and RBAC3. This component is used to apply more restriction to the system and to perform organization policy. For instance, most organization will not allow the same user having the roles of purchasing manager and the roles of account payable manager since such permission can lead to the fraudulent dealings. Constraint can be used to restrict this permission by giving some condition to the roles and hence restrict the user from getting both roles.

With respect to the figure 9 constraints can be applied to the user assignment, permission assignment and the session. The example of the constraint that is applied to the user assignment is the restriction, which the user is allowed to have only one role. It supports separation of duty. The constraint for permission assignment can be applied in the same manner like constraint applied for user assignment. For instance, the certain permission is allowed to be assigned to one role only. This method will support separation of duties. Constraint that is assigned to the session can be used to limit the number of session allowed for each user and the user can exercise the certain number of the roles only.

5. Discussion

Various methods have been used to approach how the system governs the access on their resources. DAC and MAC have been used by the people from along time ago to formalize security mechanism on the information system. DAC is known for its flexibility in implementing security mechanism, therefore it can be applied in almost all of the information system (Sandhu and Samarati, 1994). But DAC has a significant drawback in conducting security mechanism since the permissions of each user are specified and granted by system administrator (Ferraiolo and Kuhn, 1994). It makes the system has a great dependencies on the system administrator rather than the organization guidelines, therefore it creates a bigger possibility that the privilege is granted to inappropriate user.

Moreover, DAC conducts security mechanism based on the ownership of each object, so the system allows users to own an object (Castano et. al, 1992; McLean, 1994). For the users who own an object, they have all of the privilege to access that object including the privilege for passing the permission of that object to the other user. It brings a difficult situation for the security administrator to monitor system security due to uncontrolled distribution of privileges. User who does not have any privilege to access an object, still be able to access that object by getting the privilege from the other user who pass this privilege to him without any permission from system administrator. Once the user has an access to the object, system will not filter the activity done by the user to that object (Sandhu and Samarati, 1994). It can lead the users to abuse their privileges, and the system will not be able to control the information flows among the objects. Moreover, the existence of Trojan horse program which has the ability to pass the user rights without the knowledge of user also brings a significant threat to the system (McLean, 1994). An effort to extend security on DAC has been conducted by (Sandhu, 1992) with Typed Access Matrix Model, which introduces strong typing on Access Matrix Model. But it could not omit the main drawback of DAC.

Because of the vulnerability from the security breach, DAC is not suitable to conduct security mechanism over the military organization although it could be accepted in various information systems, mainly in the business organization. Military organization needs the high security assurance without compromising any risk that is possible to happen. For the military organization, MAC is more suitable than DAC since MAC offers more secure mechanism (Castano et. al, 1994; Sandhu and Samarati, 1994). In conducting security mechanism, MAC applies multilevel security labels to every subject and every object in the system. With this method MAC is able to control information flow in the system. But MAC delivers too rigid security mechanism. Instead for some military organization especially for the organization that has a large number of users and objects, it is not easy to give security label to every subject and every object in the system (McLean, 1990; Pernul, 1995; Sandhu and Samarati, 1994). In fact, the relation between user and object is conducted in many to many relations, it means a set of users deal with a set of objects. Thus, defining security label to each user and each object would bring a difficulty in updating and administering database. Moreover, the insertion of new user and new object in the system especially for those having a new security label cannot be done easily as it must consider the existing. The new assignment to the existing user also brings a significant difficulty in maintaining database. This drawback can influence the live cycle of data in the system.

The method combining DAC and MAC had been proposed by Denning (1986) with the Sea View model. In this model, DAC is represented by the TCB model and MAC by the MAC model. TCB model is layered on the MAC model. Although this model is able to solve the problem of DAC in controlling information flows, this model still carries the problem of MAC in rigidity and DAC in the relation of user and object for the same security level. Considering business organization, it almost is impossible to apply MAC in its system.

RBAC brings a new way in governing access control. This method relies on the function of each user within the organization represented by the roles, therefore it depends on the organization guidelines (Sandhu, 1997). The privileges owned by the user are limited by the roles belongs to the user. It makes the user will not be able to get more privileges than they need to do their job (Ferraiolo and Kuhn, 1992; Sandhu, 1997). Moreover, RBAC supports separation of duties for each user following the roles owned by the user. But this method has a drawback in handling multilevel data since the user is not connected directly to the access permission. The relation of user and permission is mediated by the roles. Therefore the definition of privileges by the roles will be resisted by the security level of subjects and objects. Although this method delivers a good security mechanism for large organization in business environment, it makes RBAC not recommended for military organization. However it reduces the flexibility of RBAC.

The other drawback of RBAC is the incapability in controlling information flow. There is a possibility that the user get an inappropriate role by collaborating with system administrator. Once the user gets this role, he can access the data following the role without any restriction.

The comparison of three-access control method can be shown in table 1.

Table 1. Comparison of DAC, MAC and RBAC

No	Security points	DAC	MAC	RBAC
1.	Basis of access request permission	Authorization list	Security level	Role
2.	System dependency on	System administrator	Classification level of subject and object	Function of user within the organization
3.	Distribution of authorization	Uncontrolled	Controlled	Controlled
4.	Object owner	System and user	System only	System only
5.	User capability to grant an access to the others	Permitted	Prohibited	Prohibited
6.	Control of information flow	No	Yes	No
7.	System maintenance and updating	Easy	Difficult	Easy

6. Conclusions

User access control govern the access request of each user in a certain method depend on the requirement of the system. There is no method better then the others. Each method has the specific strong points, on the other hand it also carries the weaknesses. To determine which access control is more suitable to be applied in the information system need the analysis on the requirement of the system.

Currently information system is implemented following the organization structure. Whatever the type of that organization, whether it is a military or business, security must be applied to protect data in the system and the system itself. The flexible method as represented by DAC is easy to be adopted, but it does not guarantee that the security mechanism brings enough protection to the system due to the weaknesses of that method. On the other hand, the very tight protection as represented by MAC will bring difficulties in implementation and maintenance of the system itself. It even can leak the existence of the over all system. RBAC has the other approach in implementing security. It brings flexibility and on the other hand carries a more secure mechanism than DAC. However, it is still not adequate to be adopted for military organization.

The idea of bringing flexibility to the military organization as well as bringing military security to the business organization still needs to be followed up. The integration of security method that can be applied in any system regardless it is a military or a business organization needs to be discovered in further research in order to cover the varying system

7. References

1. Ahmad Baraani-Dastjerdi, Josef Pieprzyk, Reihaneh Safavi-Naini. Security in Databases: A Survey Study. 1996.
2. Bertino E and Ferrari E. Data Security. *Proceedings on the Computer Software and Applications Conference.* 1998.
3. Chandramouli Ramaswamy and Ravi Sandhu. Role-Based Access Control Features in Commercial Database Management Systems. *In Proceedings of NISSC'98.* 1998.
4. David Ferraiolo and Richard Kuhn. Role Based Access-Control. *Proceedings of 15th National Computer Security Conference,* 1992.
5. David Ferraiolo, Janet Cugini and Richard Kuhn. Role Based Access-Control (RBAC): Features and Motivations. *In Proceedings of 11th Annual Computer Security Conference.* December 1995.
6. D.E. Denning. Cryptography and Data Security. *Addison-Wesley.* 1983.
7. Günter Pernul. Information Systems Security: Scope, State-of-the-art, and Evaluation of Techniques. *Int. Journal of Information Management,* Vol. 15, No. 3, Butterworth-Heinemann, June 1995.
8. Halim. M. Khelalfa. Computer Security Inference Control. http://mirror-us.unesco.org/webworld/public_domain/tunis97/com_54/com_54.html. May 1997.
9. John McLean. A comment on the "Basic Security Theorem" of Bell and LaPadula. *Information Processing Letters 20.* 1985.
10. John McLean. The Specification and Modeling of Computer Security. *Computer, vol. 23, no. 1.* January 1990.
11. John McLean. Security Models. *Encyclopedia of Software Engineering (ed. John Marciniak), Wiley and Sons, Inc.* 1994.
12. Kioumars Yazdaniam and Frederic Cuppens. Neighborhood Data and Database Security. *Proceedings on the 1992-1993 ACM SIGSAC on New Security Paradigm Workshop.* August 1993.
13. MD. Rafiqul Islam. Design and Analysis of a Dynamic Access Control Scheme. *Universiti Teknologi Malaysia PhD Thesis.* April 1999.
14. Micki Krause and Harold F. Tipton. Handbook of Information Security Management. *CRC Press LLC.* 1999.
15. Mukesh Singhal and Nirajan G. Shivaratri. Advanced Concepts in Operating Systems: Distributed, Database and Multiprocessor Operating Systems. *McGraw-Hill.*1994.
16. P. Ammann, S. Jajodia and I. Ray. Ensuring Atomicity of Multilevel Transactions. *Proceedings of the IEEE Symphosium on Research in Security and Privacy.* 1996.
17. Ravi S. Sandhu. The Typed Access Matrix Model. *Proceedings of IEEE Symposiums on Security and Privacy,* Oakland, California, May 4-6, 1992.
18. Ravi S. Sandhu. Lattice-Based Access Control Models. *IEEE Computer,* Volume 26, Number 11, November 1993.
19. Ravi Sandhu. Role-Based Access control. *Proceedings of 10th Annual Computer Security Applications Conference.* 1994.
20. Ravi S. Sandhu and Pierangela Samarati. Access Control: Principles and Practice. *IEEE Communications Magazine,* September 1994.
21. Ravi Sandhu. Role-Based Access Control: A Multi-Dimensional View. *Proceedings on 10th Annual Computer Security Applications Conference.* December 1994.
22. Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman. Role-Based Access Control Models. *IEEE Computer,* Volume 29, Number 2, February 1996.
23. Ravi Sandhu. Role Hierarchies and Constraints for Lattice-Based Access Controls. *Proceedings Fourth European Symposium on Research in computer Security.* September 25-27, 1996.

24. Ravi Sandhu, Venkata Bhamidipati. The ARBAC97 Model for Role-Based Administration of Roles: Preliminary Description and Outline. *Proceedings of Second ACM Workshop on Role-Based Access Control.* 1997
25. Ravi Sandhu. Role Activation Hierarchies. *Proceedings of 3rd ACM Workshop on Role-Based Access Control*, Fairfax, Virginia, October 22-23, 1998.
26. S. Jajodia. Database Security and Privacy. *ACM Computing Surveys 50th Anniversary Commemorative Issue.* March 1996.
27. Silvana Castano, Maria Grazia Fugini, Giancarlo Martella, Pierangela Samarati. Database Security. *Addison Wesley.* 1994.
28. Thomas Y. C. Woo and Simon S. Lam. Authorization in distributed Systems: A Formal Approach. *Proceedings of the IEEE Conference on Security and Privacy.* 1992.
29. Vijay Atluri, Sushil Jajodia, Tom Keefe, Cathy McCollum and Ravi Muhkamala. Multilevel Secure Transaction Processing: Status and Prospects. *Database security X: Status and Prospects.* 1997.