I. J. Computer Network and Information Security, 2013, 5, 19-29
Published Online April 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.05.03

Criteria Specifications for the Comparison and Evaluation of Access Control Models

Shabnam Mohammad Hasani, Nasser Modiri
Department of Computer,Zanjan Branch,Islamic Azad University,Zanjan,Iran
shabnam.mhasani@gmail.com

Abstract **—** Nowadays, information systems cover all-important aspects of people's life, and computer applications are vastly used in widespread fields from medicine to military sector. Because of considerable dependence on computer-based systems, the security of the information saved in these systems is of great concern, and therefore, the complexity of data protection and availability of many modern systems are increasing. Access control is considered as the core of information security and the center of data protection and availability of needs. In the organizations, whose operations require the share of digital resources with different degrees of sensitivity, such an access control is crucially required. Considering the diverse structure, requirements, and specifications of an organization, and taking into account that access control policies and models are available in diverse forms, it is required to select and implement an appropriate access control model consistent with the security requirements of the related organization in order to achieve the best results and minimum access risks and threats. In this paper, the main and most important criteria in the different access control models are evaluated and finally, the most appropriate model is introduced for implementation based on the security policies and requirements of organizations and the specifications of each access control model.

Index Terms **—** Access Control Models,Criteria, Evaluation ,Information Security

I. INTRODUCTION

One of the most important aspects of today's systems is to protect their resources (data and services) against unauthorized disclosure (confidentiality) and unauthorized intentional or unintentional modifications (integrity), as well as to ensure their availability to the authorized users when required. The sufficient security of information and information systems is an important managerial responsibility; therefore, all applications, whether of financial, security, business, or defense nature, are equipped with the different types of access controls.

Access control is an activity ensuring that only authorized users have access to items and not more. The development of access control system required regulations to be defined for access controls and implementation of applicable controls. This development is initiated based on a multistage approach using the concepts of access control policy, access control model, and access control mechanism. Policy defines high-level rules for the regulation of the type of access control; in other words, access control policies are high-level requirements that show how access is managed, who is permitted to have access to information and under which conditions such access is provided.[1] Access control policies are implemented by mechanisms that translate user's access requests in a form acceptable to the system.

Access control mechanism defines the low-level (hardware and software) operations representing the controls imposed by policies and displayed formally in access control model. [1]

Access control model acts like a bridge between policy and mechanism to describe the security properties of access control system. Indeed, security models are a superficial representation of the security policy implemented by the system, and suitable for proving theoretical constraints.

Access control model provides a formal representation of the security policy for access control and its works. Such formalization stabilizes the security properties designed by access control system. [1]

In this paper, the main criteria and properties supported by access control policies and models are explained, and then their effects on the quality criteria of access control models are studied. For this purpose, we firstly explain the concept of information security, and then access control models are studied, and important criteria and properties of these models are introduced and evaluated.

II. INFORMATION SECURITY

Here, the[2] has been used for the classification of information security that provides three main important security services:

-Confidentiality**:** this aspect of security ensures that information is only provided to the authorized users.

-Integrity**:** this security service protects the accuracy and integration of information and information is protects against any modifications.

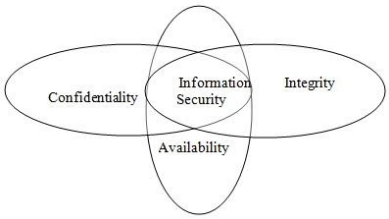

Figure 1: Information Security Principle

-Availability**:** means that information or its resources must be available to authorized users whenever required. Fig 1 shows the information security principle.

2.1 Security Models

In general, security models are as follows:

2.1.1 Bell – La Padula (BLP) model [3,4]

In 1973, David Bell and Len Lapadula introduced a model that provided a mathematical description for security policies. During the past three decades, this model has been the strongest security model. The concepts of this model include subject, object, and reference monitor. BLP model determines access to reading and writing between subject and object based on the dominant relation between subject label (access class) and object label (access class). Reference monitor is the core of operating system and an abstract interface machine between the access of subject and object and it has control and monitor over all accesses. Security label shows the sensitivity level of information and authorized level of subjects. The security policy of this model prevents the flow of information with "top secret" label to the information labeled "unclassified". Therefore, this model is categorized as a general model of mandatory access control policies and it focuses only the security service "confidentiality", but not integrity. Suppose that S is a set of subjects and O is a set of objects in a system. The label C(S) is attached to any existing subject in the set of subjects, and any object in the set of objects receives the label C(O) as the class of access. The subject can read the object if c(s)>= c(o), and only in case of c(o)>= c(s), the subject is authorized to write on the object. This model uses the security characteristic Simple Security Property and * - Property.

- Simple Security Property**:** This characteristic indicates that no subject is authorized to have access to the information at a higher security level (NO READ UP).
- * - Property**:** This characteristic prevents a subject to write on an object at a lower security level (NO WRITE DOWN). If the subject S reads the object O, then it can write on the object P, only if c(p)>=c(o).

2.1.2 BIBA Integrity Model[4]

As mentioned, BLP model describes methods that guarantee the confidentiality of information flow. Accordingly, the model introduced by Biba is a model similar to BLP, but focusing on the integrity of information, and it ensures that the data do not flow from a resource with low integrity to the one with high integrity. This model solved ultimately the problem of unauthorized modifications by constraining reading and writing. For this purpose, the levels of integrity are determined by assigning the labels of "high" and "low" to subjects and objects. For example, the objects with the label of "high" are highly integrated, and a subject is permitted to read the objects at a higher level of integrity, but it is only authorized to write on the objects labeled "Low". In BIBA model, subjects and objects are ordered based on their integrity level (label). We assume I(s) as the integrity level of the subject s, and I(o) as the integrity level of the object o. A subject is permitted to modify the object o, only if I(s) >= I(o) (NO READ DOWN); and if s is authorized to have access to the object o at the integrity level of I(o), the subject s is permitted to write on p, only if I(o)>=I(p) (NO WRITE UP).

2.1.3 Chinese wall Model

This model was introduced by Brewer and Nash in 1989 focusing on the conflict of interest. This model combines mandatory and discretionary elements and it includes both confidentiality policies and integrity ones.[4] The elements of Chinese wall model include subjects, objects, data set, conflict of interest classes, and labels. The main concept introduced by this model is that the users are not permitted to have access to the confidential information existing in the client of an organization and its competitors. No-wall users are initialized and in case a file is available, the files containing the information of the competitors are converted to unavailable. In contrast to other models, the access control regulations of this model are changed based on the behaviors of user, and the access rights of user are specified dynamically.

In this model, data sets are categorized into different classes of the conflict of interest, and all subjects have access to at most one set of data at any class based on mandatory regulations. The policy of this model determines that a subject is only authorized to have access right if the requested resource is in the data set, to which the related subject has always access, or in case the related resource does not belong to the classes of financial conflicts of interest accessible to the subject. [5]

2.1.4 Clark–Wilson Model

This integrity model has been provided to meet the security requirements of business plans and it focuses on the transactions carried out over objects. In this model, the conditions of the systems before and after transaction must be consistent with each other. This model focused on integrity and has two types of integrity including 1) internal integrity, 2) external integrity. The mechanisms of implementing integrity are based on well-formed transactions and separation of duty. In this model, subjects and objects are labeled using programs, which acts like interfaces between

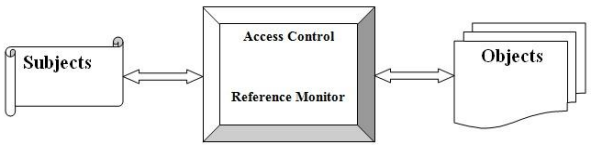

Figure 2: Access Control Principle

subjects and objects. Access control in this model defines access operations conducted on any type of data and access operations conducted by subject. The different of this model from BLP is that BLP model is based on a multipurpose system, but Clark – Wilson model on an applied program.

III. ACCESS CONTROL

3.1 Definition of Access

Access means the interaction between a subject and an object(Fig 2). For example, a subject can read an object or write on an object; and in some cases, an object can be used without reading or writing process (execution).

3.2 Definition of Access Control

Access control is a set of policies and measures for granting or revoking the permission to a specified user for having access, or constrained access to the resources of an information system accessible to users, programs, processes, or other authorized systems. [1]

The main task of access control is to control the access of users to a system and its resources in such a way that only authorized access is possible. Access control determines if the request for access to the related system is accepted or rejected. These decisions on access control are based on access control policies of the system, and are executed by access control mechanisms.

3.3 Concepts of an Access Control System

3.3.1 The Elements of Basic Access Control Model

3.3.1.1 Subject

In an access control system, subject means a set of active entities requesting for having access to objects. In different access control models, entities (including individuals, processes, or machines) can execute operations in the related system to flow information between objects or modify the situation of a system.

3.3.1.2 Object

Object is a set of passive entities of a system (resource) that are accessed and must be protected. In other words, objects are entities containing or receiving information, indicating the resources of a system and to which access must be controlled or constrained. Access to an object means access to its information. Objects include records, fields, pages, segments, programs, keyboards, printers, and network nodes. Moreover, the devices connected to the network including switches, routers, and mechanical elements are considered as objects.

Subjects and objects are software entities and are used instead of human users, and any human user affects the system by controllable software entities.

3.3.1.3 Access Method and Rights

Access rights mean the different methods used by the subject for executing operations such as reading, writing, and execution, on the objects authorized for access.

In this process, a subject request for access, reference monitor decides to accept or reject the request of access.

3-3-1-4 Operation

Operation is an active process requested by a subject. For example, when a user inserts his card into ATM and inserts the pin code, a control operation is carried out.

3-3-1-5 Privilege

Privilege, which is a combination of object and operation, is a permission for conducting an operation in a system. A specified operation run on two different objects is regarded as two different permissions. Accordingly, two operations conducted on an object represent two different permissions.

Fig 3 shows the access control elements.

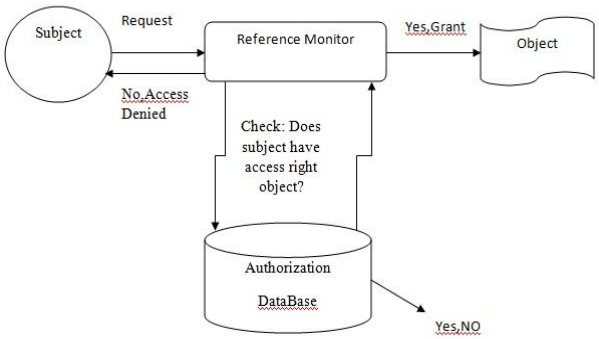

Figure 3: Access Control Elements

3.3.1.6 Need to Access Control

The concept of access control in information security is not a side issue, rather it is used to set constraints such as least privileges, and need-to-know for meeting organizational security policies.

3.4 Implementation of Access Control System

In general, there are three crucial concepts in an access control system as follows:

1) Access control policies
2) Access control models
3) Access control mechanisms

3.4.1 Access Control Policies:

Policies that are high-level rules state that, who has access to which information under which conditions and method. Access control policies are classified as follows[4].Fig 4 shows the access control policies classification.

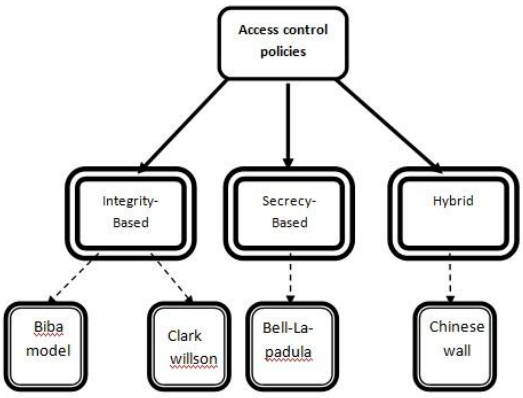

Figure 4: The Classification of Access Control Policies[4]

3.4.2 Introducing Access Control Models:

Access control model is a framework showing how a subject has access to objects. Access control models specify rules that determine how people can have access to resources to consider confidentiality and integrity, and auditing of users. Access control models can be classified into traditional and developed groups. In traditional group, there are two mandatory and discretionary access control models, which are regarded as basic models. Developed access models are indeed those ones based on traditional models, which have been developed, and whose problems are removed.

Access control models facilitate access control decisions and determine how a system is protected and access to resources is managed. Access control policies are classified into two groups of discretionary and non-discretionary policies in terms of objective. In discretionary policies, resource is responsible to issue access permission. This issue improves the capability of these policies and reduces in contrast their security. Discretionary policies are implemented by direct and explicit such as access control list (that maps specified users to specified resources)[6]. In contrast to discretionary policies, there are non-discretionary ones, in which access is permitted by administrator in accordance with predefined rules. Access policies are configured by the language of policies using access control mechanisms[6]. Access control models act like a bridge between real policies and mechanisms for their implementation. Any model has its own mechanism and is able to meet the different access needs from different aspects[6, 7]. As models have vast use, no clear border can be depicted to separate their usage domain. The development of access control begins with the definition of security policies, and it requires knowledge regarding resources, users, and security subject. Any special security requirement must be recognized for the management of special conditions. Therefore, an appropriate access model can be selected and configured together with security policies. To support the functions of models, mechanisms are required, and factors such as migration costs and user's interests help to select the proper model. [6]

3-4-2-1 DiscretionaryAccess Control Model(DAC)

Discretionary Access Control **(**DAC) policies exercise access controls based on the user's identity (ID) and explicit access rules stating that who is permitted to conduct what on a resource[5]. In DAC, network administrator permits the subjects holding resources to decide on accepting or rejecting the access to the resources at their sole discretion. This access control model is based on the data owner and subject has required authority with certain constraints to determine which objects are accessible. Data owner is the user who created the related file. This model is welcomed in public sectors and business organizations. Linux – UNIX windows is an operating system based on this access control model.

3-4-2-1-1 Implementation Mechanism

Access control matrix, access control list, and capability list are used as the mechanisms for the implementation of this model.

3-4-2-1-2 Access Control Matrix

Access control matrix is a two-dimensional matrix used to control the access permission given to a subject to have access to an object. In other words, this is a table, in which any row corresponds to a subject and any column to an object (files, devices, resources, and services). Each matrix entry is a set of access rights given to a subject for having access to any object.

3-4-2-1-3 Access Control List

This mechanism is a list of controlled access permissions as regards a resource, and a list of all subjects, who are permitted to have access to that object (resource) based on their access rights. Each entry in the list is in form of an ordered pair (subject and access right). Access control list can be used to judge about the authorized accesses to objects, who have access to the system, and which access permissions they have. As access control lists are simple and practical, they can be implemented in many modern operating systems directly or indirectly.[7]

3-4-2-1-4 Capability List

This is a list of access permissions of users and a list of all objects, to which these users have access based on their access rights. [7]

3-4-2-2 Mandatory Access Control Model

Mandatory access control model (MAC) is a strict and structured model, in which the final decision on access is made by the operating system. The decision made by the operating system dominates the requests of users. In mandatory access control model, the decisions of access control policy are made by a central administrator, not by the object owner. Therefore, the owner cannot modify the access rights. This model is based on security label, an all users have their own security clearance label (top secret, secret, and unclassified). The Objects are also classified into confidential, public, and private based on the sensitivity

of the information that they contain. The clearance and security sensitivity of both elements are saved in security labels and the final decision will be made based on subject clearance, security sensitivity, and security policy. Protective decisions are made only by the system, and the owners of objects are not permitted to intervene. A user receives access permission only if his security clearance interval is greater than or equal to the security sensitivity level of the related object.

This model is used in the systems with multilevel classifications and mostly in military and intelligent sectors for keeping access policies. This model is implemented based on the security labels of subjects and objects. These labels are required for the implementation of the security policies. MAC model depends on multilevel BLP security model, and BIBA model. However, as MAC model is based on confidentiality and BLP security model on the security aspect of confidentiality, BLP model is used more, and as BIBA model focuses on integrity, it is less used. [8]

3-4-2-3Role-Based Access Control Model (RBAC)

In this model, roles are used for the management of permissions issued for enforcing security policies. RBAC is role-based and has a central administrator and a set of roles determining who users are permitted to have access to resources. Access rights are grouped based on role's names, and the membership right of the roles is based on the abilities and responsibilities of users in the organization. Therefore, membership can be easily added or deleted. This model is free of the complexity of very large access control policies, and makes the administration of access control very easy. One of the advantages of this model is that it supports UNIX groups and is a combination of the properties of DAC and MAC, and as it is more general than MAC and DAC models, it can be customized for each program. RBAC is to some extent based on BIBA model, and suitable for the organizations with higher personnel shift.[6,8]This model is used in operating system, database, and system management. The main challenge of this model is the competition for the provision of a strict security and simplicity of administration. The simplicity of administration here means that a few roles assigned to the users working with several roles are managed, as the assignment of several roles to a user is the main cause of internal threats and endangering of security.

3-4-3 Access Control Mechanisms

These mechanisms have been explained in details in the section on the implementation mechanisms of access control models.

IV. CRITERIA FOR THE COMPARISON OF ACCESS CONTROL MODELS

In this section, the criteria used for the comparison and evaluation of access control models are studied. For this purpose, these criteria are classified into two general groups: 1) quality criteria, 2) basic and main criteria.

4-1Quality Criteria

In access control models, the main purpose is to select the model, which is sufficiently expressive, meaningful, and flexible enough for meeting security needs and the requirements of access control of the different organizations. Moreover, another important issue is that an access control model is required to answer two main questions on efficiency level and scalability. If the model cannot be expanded easily, this program will be questionable in the real world. Moreover, the development of the model should not affect its efficiency negatively.

4-2 Basic and Main Criteria

Nan Zhang [9] provided the following basic criteria in his thesis for the comparison of access control models. After introducing the following criteria, we study the role of each criterion on the access control models and their effects on the quality criteria.

4-2-1 Administrative Policies

Administrative Policies are the policies that defining who can add, delete or modify the policies. Some researchers call them meta–policies, or, permissions about permissions. The careful definition of administrative policies is important to any access control system, since if they are not exactly specified, the whole system might lose the fore of protection. Therefore, any access control model must address the issue of how administrative privileges are organized. There are four main types of solutions in this regard:

- Centralized solution: where a user or a group of privileged users, known as administrator (s) retain the privileges of granting or revoking permissions.
- Hierarchical solution: where the administrator power is distributed among a set of authorized users.
- Ownership: where the owner of an object can grant or revoke from other users the permissions for having access his objects.
- Decentralized solution: where the administrative power is further distributed among common users through delegation.

Fig 5 shows this principle, over-centralized solutions should be avoided by any model as they may cause root-bottleneck problem as well as the misuse of administrative power. Moreover, over-decentralized solutions should also be avoided because they may complicate the authorization management, and users may find that it is difficult to keep track of who can access their objects.

Administrative policies determine who can add, delete, or modify access control permissions. In primary access control models, there was centralized access control, but in distributed and collaborative environments, it is important to have a decentralized

approach in order to transfer the role of administration to specific users.

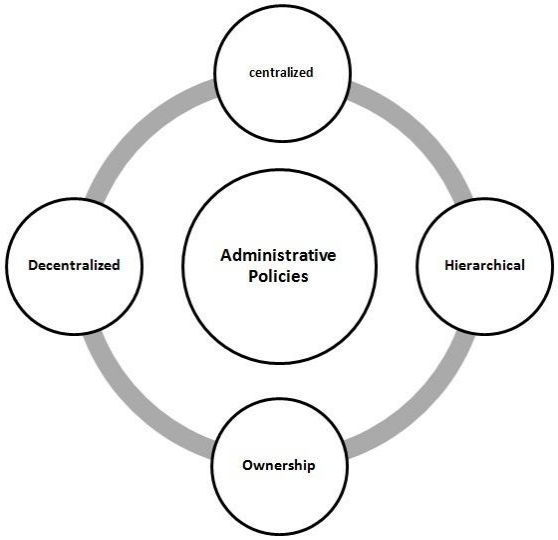

Figure 5: The Classification of Administrative Policies

4-3 The Comparison of the Criterion Administrative Policies in Access Control Models and Its Effects on the Quality Criteria of Access Control Model

4-3-1The Role of Administrative Policies Criteria in DAC:

As mentioned, DAC policies are based on user's identity (ID)and explicit access rules, stating that who is authorized to do what on which resource[10]. Here the grant or revocation (GRANT/REVOKE) is based on the identity of the subject, and this ID can be user's identity or membership in a group. One of the advantages of this method is that this model is flexible due to its little dependent on administrator, and as the administrator of network authorizes the owners of resources to control the access of the owners to their files[6]. Decentralized control enables users to have dynamic access to information. However, one disadvantage of the administrative policy existing in this model is that users are permitted to have control over access permissions issued for the access to financial resources, and this makes a system vulnerable against the attacks of Trojan horse.[8]

4-3-2The Role of Administrative Policies Criteria in MAC:

In this model, policies for having access to an object are determined by an individual superior than the owner and the creator of the object, rather by one or several security mechanisms in the system. A user, who is even the owner of an object, cannot modify the control policy of access to that object. Moreover, user's processes are not permitted to modify policies. In this model, access control policies are determined by the owner, developer, or custodian of the system[4]. Mandatory control policies or lattice-based access controls are those policies, in which individuals have no role in making decisions on the access of others to information, and access control policies are specified by a central administrator based on mandatory regulations in a centralized manner[10, 11]. Moreover, information flows in a channel protected by security labels (in a bottom – up manner and not top – down). One disadvantage of this model is that the assignment of security labels by the administrator of the system causes constraints in the operations of the user and this reduces its flexibility. [12]

4-3-3The Role of Administrative Policies Criteria in RBAC:

Administrative policies in this model use roles for the management of permissions issued for access control. This model is welcomed by applications such as Oracle. It is called non-discretionary as the access decisions are made based on the rights and permissions of each role or groups. Access control policies are based on two things: firstly, the roles received by the users; secondly, the regulations that determine which accesses are permitted for that role[12]. System administrators create roles and groups, and assign rights and permissions to the roles instead of users. When a user is granted a role, all rights and permissions of such a role is inherited by the user that is the user receives the permissions implicitly.

4-2-2Constraints

Constraints are secure instructions that should be followed by the policymakers. Constraints are as follows:

4-2-2-1Separation of Duty

One constraint exercised in most organizations is the separation of duty and it means that the privileges shall not be so vested to only one person that he can damage the system. For example, in a company, purchasing manager or accounting managers shall not regarded as a person. It seems that one individual cannot commit a critical action leading to damage to an organization. The use of separation of duty reduces considerably the likelihood of violation and security offences. Therefore, an access control model should be so flexible to model the requirements of separation of duty.

One of the most basic policies of access control is to prevent unauthorized access to information. For example, individuals are permitted to have access to objects that are related to their duties. This type of control requires constraining the access to objects to a limited number of users. The policies of separation of duty are used vastly in business, industry, and governments. They are classified into three basic groups of policies: static, dynamic, and history – based separation of duties. Different access control mechanisms support different requirements of separation of duty. Usually, access control mechanisms demonstrate flexibility and efficiency in assigning properties to objects and individuals. The characteristic of separation of duty is measured by counting the number of the different types of separation of duty (static, dynamic, and history-based) that are supported

by a system, such as the stages required for the separation of the users of the groups A and B from the objects of the groups X and Y.[13] This characteristic of access control requires that no user have sufficient privilege to endanger the security of a system. For example, root privilege in UNIX operating system provides one user many privileges to conduct many security operations. As a result, there is a weak point for security of the system leading to security violations.[14,15] Therefore, access control model is to be so flexible that model the requirements of separation of duty.

4-2-2-1-1 Types of Separation of Duty:

The separation of duty has two types, Static or strong exclusive, and Dynamic of weak exclusive.

Static Separation of Duty:

The static separation of duty states, "A principal may not be member of any two exclusive roles". This means that the user is authorized of one role may not be authorize of another role or two roles have no any shared principle. Static policies assign duties to the users without saving the history of the related duty. If static separation of duty implements policies, the concept of separation of duty has been implemented too.

Dynamic Separation of Duty:

The Dynamic separation of duty states, "A principal may be a member of any two exclusive roles, but it must not activate them both at the same time". The above definition shows that user is authorized of both roles but both roles cannot be active at the same time. It means system will keep the record of each task. In this record, all the information that is used is to be performed. Before doing any task, the system will check the separation of policy should not to be broken. Weak exclusion, or Dynamic Separation of Duty, provides the larger set of possible policies, which control the commencements and use of roles.[12]

Comparing Static and Dynamic types of the Separation of Duty:

The comparison of these two types of the separation of duty reveals that static type is more suitable for the analysis and definition of system, while the dynamic type is not so as it is more flexible, for it makes it possible to protect the system based on adaptability.

History-based Separation of Duty:

Two and more limited roles may have common members and the union of the action granted by those roles may distance the action in the business task, but no role member is allowed to perform all the actions ascendancy the business task on the equivalent target or collection of target called as history based separation of duty.

Separation of Duty in DAC

As mentioned, the control of access to resources in DAC is vested to the owner of the related object. However, this model has problems of integrity, such as least privileges and separation of duty.

Separation of Duty in MAC

MAC model does not support (dynamic) separation of duty.

Separation of Duty in RBAC

RBAC model uses constraints to implement separation of duty. Separation of duty among users assigned a specific duty prevent him from performing any other duty[16].

4-2-2-2Definition of Least Privilege

This principle means that a subject of a system should only be permitted to have access to the least privileges that are required for performing to the user's duties. For this purpose, it is required to determine policies statically and implement them dynamically.[14,15] Fine-grained access control vests access control to those entities that require having access. In dynamic condition, the principles of least privileges are applied by limited processed that are constrained for performing operations within the framework of the limited privileges. Any user and process must be enjoyed only of the least privileges that are required for performing duties. It must be noted that the application of these principles reduces the results of system error or harmful events.

Least Privileges in DAC

According to the facts mentioned in the previous sections, it is clear that this model can apply the principles of access with least privilege. [8]

Least Privileges in MAC

According to the facts mentioned in the previous sections, it is clear that this model cannot support the concept of least privilege.

Least Privileges in RBAC

This model supports least privilege, separation of duty, centralized administration of access control and roles.

The Role of the Criterion Constraint in Quality Criteria

The criterion constraint is effective in the expressiveness of model. The challenge provided by constraints in each model is that if the model is sufficiently meaningful and expressive to display different constraints.

4-2-3Delegation

Delegation is a mechanism of administration and the process, upon which a user, who is not benefited from administration privilege, is empowered to grant others with permissions.[17] In public access control models, user access rights are predefined. In some cases, users need new access privileges due to the dynamic nature of their activity. To meet this need, there are two solutions: 1) system administrator grants the user access right based on user's needs; 2) the user is granted access right by any other user. The second process is called delegation, which means the capability of a subject to delegate his privileges to any other user partially or totally. As a result, the delegated user is empowered to

perform the activities of the delegating user. This concept has been subject to many studies and discussions in security policies. [9]

4-2-3-1The Role of Criterion Delegation in Quality Criteria

The correct and appropriate use of delegation increases the flexibility of access control system. Zhang provides three reasons for such flexibility: 1) by delegation, a subject can perform the duties of another subject in case of the absence of the latter; 2) by delegation, the process of authorization is decentralized, since the presence of an administrator in a system to assign users their access rights reduces efficiency; 3) delegation is proper for the environments, in which users cooperate for the performance of a common task. For instance, an owner of a file authorizes other users interested to read the related file by delegation. The incorrect use of delegation may happen when a security risk is present. For example, an administrator may grant by delegation some privileges that have not been given to any user, to some individuals who are not liable to such privileges.[9,18]

Moreover, root-bottleneck may happen in case of delegation. Moreover, the application of the concept of delegation in an access control system, some other concepts may become complicated. The concepts such as revocation may get more complexity in multi-step delegation and this complexity lead to some problems in security terms. By delegation, some privileges may be delegated to the users that are not authorized to receive such privileges. Moreover, delegation may break down some main constraints. Therefore, it is required to ensure that delegation behaviors are consistent with other regulations and constraints in the models that are benefited from delegation mechanisms. The quality criteria regarding delegation include totality, permanence, monotonicity, level of delegation, and revocation. In delegation terms, permanence refers to the duration of delegation. In many cases, delegation is applied temporarily, and it is revoked after its expiration time. In monotonic delegation, the grantor of privileges maintains the permission he has delegated. On the other hand, with a non-monotonic delegation, the grantor loses the permission for the duration of the delegation. Level of delegation specifys whether or not each delegation can be further delegated and how many times. The method of revocation is another criterion that has an important role in delegation. [9, 17, 18]

4-2-3-2Delegation in DAC model

As in this model, the owner of the system determines how the resources are accessed by others, therefore the owner can grant some of his privileges by delegation easily.

4-2-3-3Delegation in MAC model

In this model, delegation is not possible due to the centralized administration and predefined access rules.

4-2-3-4Delegation in RBAC model

The issue of delegation and its revocation in this model has not been studied (decentralization of administration); moreover, central role is accountable for control in most suggestions. [12]

4-2-4 Mechanisms

In general, mechanisms have been explained in the introduction of access control models. The following criteria have been provided by Saad Zafar, Sabrina de Capitani di Vimercati, Pierangela Samarati, and Sushil Jajodia.[14,19]

4-2-5 Conditions[15,19]

In general, three types of conditions are supported in access control models: system-dependent conditions, content-dependent conditions, and history-dependent conditions.

In system-dependent conditions, authorization is validated based on the consent of the predications of the system such as access location and time. For example, the access of the personnel of a bank to the account is conditioned to the working hours and bank premises. Content-dependent conditions are prevailed in form of access constrains based on the content of the resource. This type of conditions are imposed for making decisions on granting of access right, or limiting access to some parts of the resource (for example a subset of the related rows). This type of conditions is useful when authorization if of fined-grain nature. The third type, i.e. history-dependent conditions, is used when access is permitted based on the accesses permitted previously.

Conditions in DAC Model

As DAC model acts by the authentication of user's ID, therefore it cannot restrict access based on a specified system, time, or network communication.

Conditions in MAC Model

This model has removed some deficiencies of DAC model by imposing some executive constraints through system. In this model, constraints such as multilevel security systems, in which subjects and objects are classified in security terms, are used. Although MAC policies impose constraints more than the authentication of user's ID, MAC model does not pay any attention to the content of the request. [20]

Conditions in RBAC Model

RBAC model is similar to DAC model, except that identity (ID) is replaced by role in RBAC. Moreover, RBAC is similar to GROUP in UNIX systems. This model is not also sufficiently efficient for content information. Michael Kirkpatrick and Elisa Bertino studied in a research paper the content indicating the role of user's request in access control.

4-2-6 Positive and Negative Authentication

In general, there are two methods for presenting access control policies: open and closed policies. In some cases, there must be exceptions, since both positive and negative authorizations should be supported. Traditionally, positive and negative

authorizations are used in mutual exclusion corresponding to two classical approaches to access control, namely open and closed policies.

4-2-6-1Closed (Positive) Policy

Authorizations specify permissions issued for an access. Closed policy permits an access when there is a positive authorization for such an access, and denied it otherwise.

4-2-6-2Open (Negative) Policy

Authorizations specify denials for an access. The open policy denies an access if there is a negative authorization for such an access, and permits it otherwise. Fig 6 shows closed and open authorization.

Open policy is usually applied in those scenarios, where the need for protection is not strong, and by default access is to be granted. Most systems adopt closed policy, which, denying access by default ensures better protection. In cases, where information is in public use by default, positive authorization is enforced.

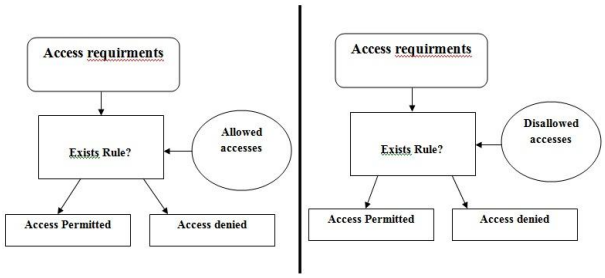

Figure 6:Closed and Open Authorization

The combined use of positive and negative authorizations is regarded as a way to support exceptions more conveniently. Suppose that we want to grant an authorization to all members of a group of thousand users except to the user Alice. In closed policy, we would have to specify a positive authorization for each member of the group except Alice. However, if we combine positive and negative authorizations, we can specify the same by granting a positive authorization to the group and a negative one to Alice. In case of combining positive and negative authorizations, the question is that how the two specifications should be dealt with.

- What if for an access, no authorization is specified.
- What if for an access there are both a negative and a positive authorization?

The first item is achieved by assuming that one of the open or closed policies operates as a default, and accordingly access is granted or denied if no authorization is found for it. It must be noted that the alternative of the fact above is too heavy, and it complicates administration. The second question is a more complex matter and does not often have a unique answer. Thus, different decision criteria should be adopted, in specific conditions in accordance with the different policies that can be implemented. An ideal access control model should support both policies and this lead to more flexibility.

Authorization in DAC Model

As DAC model uses and executes the mechanisms such as access control lists, access control matrix, and capability list, taking into account that the subject of this model is based on positive authorization, therefore, this model applies positive authorization approach.

Authorization in MAC Model

As MAC model uses security label for subjects and objects to determine the access of users to resources based on such security labels, therefore, this model supports positive authorization.

Authorization in RBAC Model

In this model, positive authorization is applied, and negative authorization is executed by constraints in RBAC2.

4-2-7 Attributed-based Specifications

In an open system such as Internet, different parties (clients and servers) interacting with each other are strangers, and have no prior relation and are not in the same security domain. As a result, the server may not have all information that it needs to decide whether an access should be granted or not on the one hand. However, the client may not know, which information he needs to provide to a server to receive access right, on the other hand. All this requires a new way of executing the process of access control that does not need to operate with a prior knowledge and return a yes/no access decision; rather, the access control process should be able to operate without a prior knowledge of the parting requesting access and return of the information of the requisites that it requires be satisfied for the access to be allowed. Also, the traditional "identity-based access control models", where subjects and objects are often identified by unique names, are not appropriate in this setting. Instead, attributes other than identity are useful in determining the party's trustworthiness. In this context, access restrictions to the data/services should be expressed by policies that specify the properties (attributes) that a requesting party should enjoy to gain access to the data and services. One of the most important aspects that should be supported by attributed-based access control policies is the ability of accesses to a set of services based on a set of attributes. [19]

4-2-8 Support of Fine-Grained vs. Coarse-Grained Access Control

4-8-1 The Definition of Graining in Access Control :

Coarse-grained access control works on large items, while fine-grained access control on smaller items. The expressiveness of the grammar used to define access control rules is of great importance, in such a way that a more flexible grammar and the information feeding it result in the fine-grained access control. For example, XACML considering about the users, resources, actions, and the environment, has a fine-grained type of access

control. RBAC implementations usually focus on the user role and target application; therefore, it is classified as coarse-grained type, as it does not focus on the activities, or other attributes of subjects or context.

Support of Coarse-Grained Access Control:

Usually access control rights, which are vested to a group of users for a set of resources, are equal. To reduce the overhead arising out of frequent specification of identical access control rights vested to a group of users and resources, it is ideal to classify them into groups. RBAC model is used for this purpose.

Support of Fine-Grained Access Control:

Although fine-grained access control for access control systems is large and complicated, it is sometimes required to use such a fine-grained control, in which the requirements of a complicated access control are treated based on individual scenarios.

By the support of fine-grained and coarse-grained access control, a vast domain of access control requirements are managed and controlled.

V. CONCLUSIONS

In this research, traditional and developed models of access control have been studied in terms of basic criteria, and the manner of affecting on quality criteria including expressiveness, flexibility, scalability, and efficiency. In the following table, the results of such a study have been provided in brief. This study and the results provided in the comparative table show that the factors affecting the flexibility of access control model include administrative policies, delegation, implementation mechanism, simultaneous negative and positive authorization, as well as fine and coarse-grained types.

Moreover, factors affecting the security of access control model include constraints such as separation of duty and least privileges that are effective in and reduce the expressiveness of the model. Therefore, it is required quality criteria including flexibility, expressiveness, security and efficiency to be consistent with each other and in accordance with the security requirements of organization. Finally, it can be concluded that a safe and

Table 1: Use basic criterias for comparing access control models

Administrative policies			
Model	DAC	MAC	RBAC
Policy type	Ownership	Centralized	Centralized
Advantage	Increasing Flexibility		Flexibility and simple management
Disavdantage	Trojan horse problem	No flexible	Hard management in large systems
constraints			
Separation of duty	Supports	Doesn't support	-
Least Privilege	supports	Doesn't support	supports
Advantage	Increasing safety	Increasing safety	Increasing safety
Disavdantage	Decreasing expressive	-	Decreasing expressive
Delegation			
	Supports	Doesn't support	Supports in distributed models
Advantage	Increasing Flexibility	-	Increasing Flexibility
Disavdantage	Increasing complexity-buttleneck problem		Increasing complexity-buttleneck problem
Implementaion mechanisms			
	Access control matrix-access control list-capability list	Subjects and objects security lables	Roles and their authorizations
Advantage	Maintenance of system and reviewing of policies are hard but the implementation is tangible and cost effective	Sutiable for multilevel classification - useful for military and intelligent enviroments	Insure integrity and availability of system. Reviewing fo security policies are simplem.
Disavdantage	Safety problem-No limitation on copy right	No flexibility-hard and expensive implementation	Administrative problem in large systems.
Conditions			
	Doesn't support	Doesn't support	Supports in distributed models
Advantage	-	-	increasing control
Disavdantage			Increasing complexity
Close and open authorization			
	Positive	Positive	Positive and negative in RBAC2
Fine-Grained and Coarse-Grained			
	Fine-grained	Fine-grained	Fine-grained

Advantage	Increasing flexibility	Increasing flexibility	Increasing flexibility
Disavdantage	-	-	-

secured access control is achieved if an optimal access control model, which is benefited from basic criteria and consistent with the security requirements of organization, is selected to meet the quality criteria.

REFERENCES

[1] D.Hau,"Unauthorized Access –Threats, Risk, and Control", Global Information Assurance Certification Paper,SANS institude, GSEC Practical Assignment, Version 1.4b, Option 1, July 11, 2003.

[2] M. Bishop,*Computer Security:Art and Science*, Boston: Addison-Wesley, 2003.

[3] D. Bell and L. LaPadula,"Secure Computer System: Unified Exposition and Multics Interpretation", TR M74-244, March 1976.

[4] G.D. Wurster, "Security Mechanisms and Policy for Mandatory Access Control in Computer Systems", doctor of philosophy Thesis, Carleton University Ottawa, Ontario, Canada,2010.

[5] David F.C. Brewer and Michael J. Nash, "The Chinese Wall Security Policy", *IEEE symposium on research in security and privacy*, 1-3 may 1989.

[6] S.Vivy, "A Survey on Access Control Deployment", *Communications in Computer and Information Science* ,2011.

[7] S. Suraj, "Design of Access Control Policy Checker (ACPC)", MS thesis, Department of Computer Science and Engineering , National Institute of Technology Rourkela, Rourkela-769 008, Orissa, India, May 2009.

[8] A. Ryan, "Methods for Access Control: Advances and Limitations", (unpublished)

[9] N.zhang, "Generating Verified Access Control Policies Through Model-Checkinga",Doctor of philosophy Thesis,2005.

[10] S. Pierangela and S. Vimercati," Access Control: Policies, Models, and Mechanisms" ,Foundation of Security Analysis and Design, Lecture Notes in computer science,Volume 2171,pp 137-196-2001.

[11] F.M. Kugblenu and M. Asim, Separation of Duty in Role Based Access Control System: A Case Study, MS Thesis ,Thesis no: MCS-2006:16, January 2007.

[12] A.H. Chinaei, "Access Control Administration With Adjustable Decentralization", Doctor of Philosophy Thesis, Waterloo, Ontario, Canada, 2007.

[13] C. Hu. Vincent, D.F. Ferraiolo and D. Ri. Kuhn, "Assessment Of Access Control Systems", Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 ,September 2006 .

[14] Z., Saad, 'Integration of Access Control Requirements into System Specfications', MS thesis, School of Information and Communication Technology Griffith University, April, 2008.

[15] S. Pierangela and S. Ravi, "Access Control Principles and Practice",IEEE Communication magazine,September 1994.

[16] H.A. Weber ,SANS Institute InfoSec Reading Room, "Role-Based Access Control: The NIST Solution", 2003.

[17]M.Ben.Ghorbel-Talbia,F.Cuppensa,N.Cuppens Boulahiaa and A. Bouhoulab," Managing Delegation in Access Control Models,IEEE,2007.

[18] Md. Moniruzzaman and K.Barker, "Delegation Of Access Rights In A Privacy Preserving Access Control Model".

[19] S. Vimercati1, S. Pierangela, and J. Sushil, Policies, Models, and Languages for Access Control, Springer,2005.

[20] M. Kirkpatrick1 and E.Bertino," Context-Dependent Authentication And Access Control".

Sh.M Hasani received her BA. Degree in computer enginnering from Islamic Azad University, North Tehran Branch, Tehran, Iran in the year 2006.Currently she is pursuing M.Sc in computer enginnering from Islamic Azad University,Zanjan,Iran under guidance of Dr Modiri. She is presently working on information security,access control and ISMS.