Review on Database Access Control Mechanisms and Models

Arpita Yadav
M.Tech
Department of Computer Science
Sanghvi Institute of Management & Science, Indore

Ritesh Shah
Assistant professor
Department of Computer Science
Sanghvi Institute of Management & Science, Indore

ABSTRACT
The recent rapid explosion of web based applications and information system have further increased the risk exposure of databases and thus, data protection is today more crucial than ever. It is more important to protect data not only from external intruders but also internal intruders. In this paper, different access control mechanisms and its models discussed to achieving the confidentiality, integrity and availability goals of the database security in the organization. The models are useful in classification systems to prevent theft of information and effect of data at higher classification levels.

Keywords
Access Control Mechanism, Bell-LaPadula security model, Biba security model, Clark Wilson model, Role Based Access Control model.

1. INTRODUCTION
The curtail data access and modification can be a risk, by which the organization can be miss lead or may miss use of the right information in against of the user or any organization.

The data security meet under the four requirements: confidentiality, integrity, availability, authenticity, these four requirements ensure the data secure from the offenders. The data should be confidential in case the data is more sensitive or important which can't be share with unauthorized user, access control mechanism refer for the confidentiality when the many user want to access the data, and the encryption technique also used for the confidentiality in distributed systems. Another aspects of the integrity, data integrity means the change of data or modify of the data, the integrity men tented by the digital signature, or access control prevent from the unauthorized user only authorized user can modify the data. The availability are that data that are available on the web, can be further strengthened by the use of techniques protecting against denial-of-service (DoS) attacks, such as the ones based on machine learning techniques[1].

Authenticity provides by the access control to particular user according to their role. Through the user can access the data, modify the data as per the role assign to them, Access control can be define in the Mandatory, Discretionary, and Role based.

1.1 Mandatory Access Control
The MAC model is based on a security system user has security authorization and resources have security labels that have data classification. This model is used in such a condition where information classification and confidentiality is very important. Whenever a subject try to access an object, an authorization rule imposed through the operating system kernel check these security attributes and finalized whether the access can take place or not.

1.2 Discretionary Access Control
The DAC model is based on the a system that uses discretionary access control, permit the owner of the object to specify which subject can access which object. this model control on the access to object based on the identity of the users who are trying to access them. It uses to separate and save from harm user from unauthorized data.

2. ACCESS CONTROL MODEL

2.1 Bell LaPadula Security Model
D.E. Bell and J. La Padula present the BLP model in 1973,[2] it focus on the data confidentiality and access control. This model is multilevel security model and used in multiple operating systems to secure the confidentiality. In this formal model, the entities in an information system are divided into subjects and objects. The BLP model is built on the concept of a state machine with a set of allowable states in a distributed system. The transition from one state to another state is defined by transition functions.

Subject can only access objects at certain levels determined by his security level. For instance, the following are two typical access specifications: "Unclassified personnel cannot read data at confidential levels" and ``Top-Secret data cannot be written into the files at unclassified levels".

The BLP model is confidentiality oriented from a defense perspective and is closed to the Mandatory Access Control (MAC) of the DoD standard.[3]

- No read-up. A subject can red only those objects whose access classes are dominated by the access class of the subject.
- No write-down. . A subject can write only those objects whose access classes are dominated by the access class of the subject.

The enforcement of these principles prevents information in a sensitive object from flowing, through either read or write operations, into objects at lower or incomparable access classes [4].

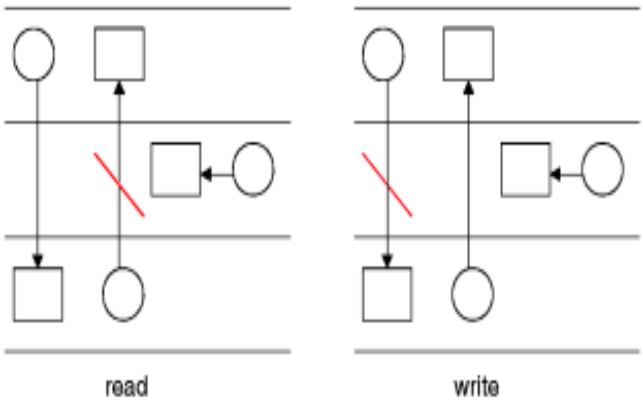

Fig. 1: BLP Security Model

Drawbacks of the BLP model

The BLP model is that it allows a given subject to write to object of higher security classification than its own classification, thus posing a threat to the integrity of the object concerned. If objects are not satisfied the required integrity level, their contents are checked to decide whether the access should be allowed. One problem of the model is that there are not any corresponding rules for checking objects contents. And another problem is that it is difficult to be realized [5].

2.2 Biba Integrity Model

The Biba integrity model was developed by Kenneth J. Biba in in 1977 at the Mitre Corporation, The motivation for creating this model is the inability of the Bell-LaPadula model to deal with integrity of data that describes a set of access control rules designed to ensure data integrity.

The Biba model defines a set of security rules similar to the Bell-LaPadula model. These rules are the reverse of the Bell-LaPadula rules:

- No read down The Simple Integrity Axiom states that a subject at a given level of integrity must not read an object at a lower integrity level.
- No write up The * (star) Integrity Axiom states that a subject at a given level of integrity must not write to any object at a higher level of integrity.

There are three main goals of integrity: Preventing unauthorized users from making modifications to data or programs. Preventing authorized users from making improper or unauthorized modifications. Maintaining internal and external consistency of data and programs.

ACCESS MODES

The Biba model has four access modes as given below.

- The modify mode permit a subject to write to an object. This mode is like to the write mode in other models.
- The observe mode permit a subject to read an object. This authority is synonyms with the read command of most other models.
- The invoke mode permit a subject to communicate with another subject.
- The execute mode permit a subject to execute an object. This mode basically allows a subject to execute a program which is the object.

Drawbacks of Biba integrity model

The model does nothing to enforce confidentiality. The Biba model doesn't support the granting and revocation of authorization. To use this model all computers in the system must support the labeling of integrity for both subjects and objects. To date, there is no network protocol that supports this labeling. So there are problems with using the Biba model in a network environment.

2.3 Clark Wilson model

The model was described in a 1987 by David D. Clark and David R. Wilson. The paper develops the model as a way to declare the concept of information integrity, The Clark-Wilson model was developed to deal with security issues in commercial environments and is primarily concerned with the integrity of data. Bell LaPadula (read-down/write-up) and Biba (read-up/write-down) model were better suited to enforcing data confidentiality rather than information integrity, Clark-Wilson model is widely used to protect commercial information against unauthorized modification. However, due to only single-level data protection support and no attention paid on difference of importance level of protected data. At the heart of the model is a triple set (CW-triples) that defines a relationship between an authenticated user and a set of transforming procedures (TPs) that operate on a set of data items. With nine constraint rules to ensure the external and internal integrity of the data items,[6]

Certification and Enforcement Rules of the Clark-Wilson Model

The following rules are from [7]: C1, C2, C3, C4, C5 are the Certification Rules and E1, E2, E3, E4 are the Enforcement Rules of the CW model.

- *C1(IVP Certification)*

  An IVP must ensure that CDIs are in a valid state when the IVP is executed.

- *C2 (Validity)*

All TPs must be certified to be valid. That is, they must take a CDI from a valid start state to a valid end state. For each TP, and each set of CDIs that it may manipulate, the security officer must specify a \relation", which defines that execution. A relation is of the form: (TPi, (CDIa, CDIb, CDIc…)), where the list of CDIs defines arguments for which the TP has been certified.

- *E1 (Enforcement of Validity):* The system must maintain the list of relations specified in rule C2, and must ensure that the only manipulation of any CDI is by a TP, operating as specified in some relation.
- *E2 (Enforcement of Separation of Duty):* The system must maintain a list of relations of the form (UserID, TPi, (CDIa, CDIb, CDIc, ….))

  Which relates a user, a TP and the data objects that TP may reference on behalf of that user. Only executions described the relations are performed.

- *C3:* The relations in E2 must be certified to meet the separation of duty requirement.
- *E3 (User Identity):* The system must authenticate each user attempting to execute a TP.
- *C4 (Journal Certification):* All TPs must be certified to write to an append-only CDI (the log) all information necessary to permit the nature of the operation to be reconstructed.
- *C5:* Any TP that takes a UDI as input must be certified to perform only valid transformations, or no transformations, for any value of the UDI. The transformation should take the a UDI to a CDI, or the UDI is rejected.
- *E4(Initiation):* Only the agent permitted to certify entities may change the list of entities associated with a TP. An agent that can certify an entity may not have any execute rights with respect to that entity.

Drawbacks of Clark-Wilson model

This model solves the problem of the Biba model, but it also has some problem as given. CW has no security level it has only integrity level. If the subjects and processes are interchangeable, a signal person could access multiple processes to violate CW simple security conditions. For solving this problem introduce the RBAC model.

3. ROLE-BASED ACCESS CONTROL MODEL

One of the most challenging problems in managing large networks is the complexity of security administration. Role based access control (also called role based security), as formalized in 1992 by David Ferraiolo and Rick Kuhn. the RBAC model consists in role creation via defining appropriate permissions. The entire procedure is performed in two stages: defining the permissions assigned to a function and providing the definitions of functions assigned to a particular role.[8]

In an organization roles provided for various job functions. Specific roles assigned to perform certain operations. staff (or other system users) are assigned particular roles, and through those role assignments acquire the computer permissions to perform particular computer-system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account; this simplifies common operations, such as adding a user, or changing a user's department.With RBAC, system administrator create roles according to the job functions performed in a company or organization, grant permission to those roles, and assign user to the roles on the basis of their specific job responsibility and qualification.RBAC is a rich and open-ended technology , which ranges from very simple at one extreme to fairly complex and sophisticated at the other.

RBAC model is defined in terms of four model components:

Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, Dynamic Separation of Duty Relations

Three primary rules are defined for RBAC as follow:

Role assignment:

A subject can execute a transaction only if the subject has selected or been assigned a role.

Role authorization:

A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.

Transaction authorization:

A subject can execute a transaction only if the transaction is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can execute only transactions for which they are authorized.

RBAC is used to protect information objects (henceforth referred to as objects) from unauthorized users. To achieve this goal, RBAC specifies and enforces different kinds of constraints. Fig. describes the general model of RBAC. RBAC has three components: base model, role hierarchies, and constraints.

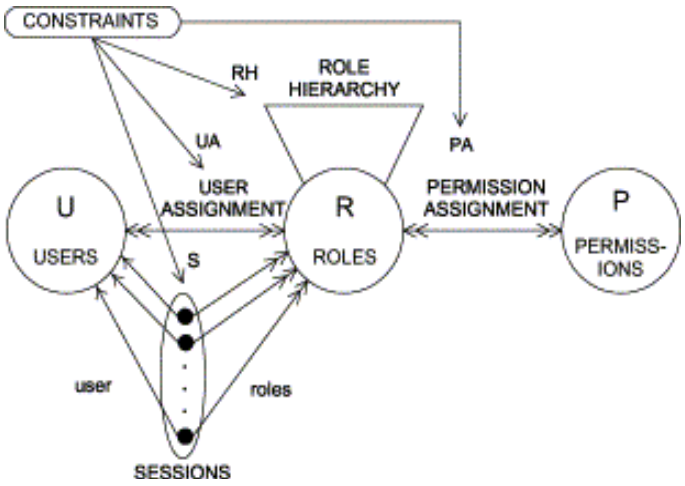

Fig. 2: RBAC Security Model

4. CONCLUSION

The need of prevent web resources and data from unauthorized access motivate access control mechanisms and security models that ensure the data confidentiality, integrity and availability. Several challenges occurred in effectiveness of security models that evacuate day by day. Role based control access model resolve the limitations of DAC and MAC mechanisms but RBAC still limited to access control in dynamic nature of relationship between users and roles. The dynamic RBAC model is suggested to remove the limitations of traditional RBAC model.

The dynamic RBAC model stills time consuming to specify the criteria between the relationships with respect to users and data items. In future, dynamic RBAC model would be focus to specify the criteria between dynamic relationships.

5. REFERENCES

[1] E. Bertino, D. Leggieri, and E. Terzi, "Securing DBMS: Characterizing and Detecting Query Flood,"Proc. Ninth Information Security Conf. (ISC '04), Sept. 2004.

[2] Bell D E, La Padula L J. Secure computer system: unified exposition and multics interpretation. Mitre Report, MTR-2997 Rev.1,1976.

[3] Trusted computer system evaluation criteria (Orange Book). Technical Report DoD Standard 5200.28-STD, U.S. Department of Defense (DoD), December 1985.

[4] Elisa Bertino, Fellow, and Ravi Sandhu,"Database Security Concepts,Approaches, and Challenges", IEEE Transactions on Dependable and secure computing, vol. 2, No. 1, March 2005

[5] "Reliability Extended Security Model Combining Confidentiality and Integrity", Xiaofei Zhang1, Changxiang Shen2 1State Key Lab of Information Security, Chinese Academy of Sciences Graduate School,Beijing 100049, P.R. China

[6] "Configuring Clark-Wilson Integrity Model to Enforce Flexible Protection", Qingui Xu, Dongguan University of technology, International Conference on Computational Intelligence and Security 2009.

[7] D.D. Clark and D.R. Wilson. A comparison of commercial and military computer security policies". In roceedings of the IEEE Symposium on Security and Privacy, Oakland, April 1987.

[8] Aneta Poniszewska-Maranda, "Representation of Extended RBAC Model Using UML Language". In Springer Berlin Heidelberg on computer science, December 27, 2004