Mandatory Access Control – Problems in it and propose a model which overcomes them

Yash Dholakia

I.T, R.G.I.T, Mumbai, India

Abstract: *The research is regarding Mandatory Access Control (MAC) which is used to specify the access for each (user) and object (data). This specifying access to both subjects and objects is done with the help of security levels. MAC is an example of Multilevel Security (MLS). There are 4 security levels in MAC. These levels include* ***top secret, secret, confidential and unclassified*** *[7]. However, these 4 security levels seem antiquated and do not seem to be in accordance with this generation's organization or business. The use of fourth security level unclassified seems ambiguous. In an organization, the people at the lowest level come under this category. However, they still have some access to organization's data or information which common people don't have. Hence there is no level for common people who can gain valuable information about the organization. This step is very important because marketing is the most important thing in this generation for an organization or a business to be successful. Without marketing, an organization cannot reach its new heights, same thing goes for business. A business or an organization can attain success by providing some valuable information to common people. Any information or data which has to be kept confidential (business strategies, employee's information, etc.) should be kept very secure and confidential. The information to be shown to be shown to common people may include its goal, its rankings nationwide or worldwide and so on.Thus, a newer version of mandatory access control must include this feature of providing some information to anyone and at the same time keeping confidential information or data very secure. Problem analysis describes this problem in detail.*

Keywords: Mandatory Access Control, Organization, Filtration, Polyinstantization.

1. Introduction:

1.1 Background review:

In order to make an organization's data secure, 3 security goals have to be satisfied. These security goals include [7]

- Confidentiality
- Integrity
- Availability

Confidentiality means that organization's data cannot be accessed by some unauthorized person. The valuable information has to be kept secure from such unauthorized access. Integrity deals with consistency, validity and accuracy of data or information of an organization [3]. It means that any unauthorized person should not be able to modify data which results in inconsistency, invalidity and inaccuracy of data and eventually loss of integrity. Availability means that data should always be available for authorized users and at the same time ensure security of data from unauthorized access. There should not be denial of services for authorized person. It should be able to access data anytime he wants. Confidentiality can be ensured by using

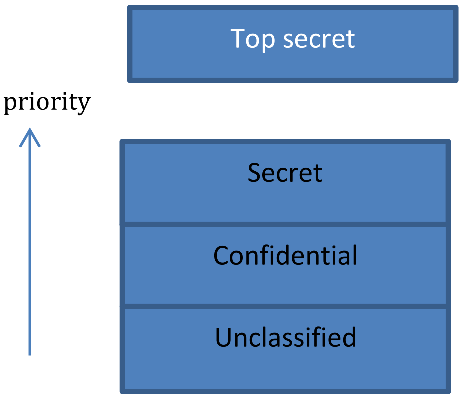
- Encrypting data of organization [3]
- Authentication [3]
- Access control [3]

Encrypt data to protect it from unauthorized access. Authentication means providing passwords, token authentication or biometric identification [12]. Access controls are of following types

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control(RBAC)

DAC is based on granting and revoking privileges. The owner of the relation grants and revoke privileges like create table, insert, delete, update to different users [7]. In RBAC, DBA (database administrator) assigns different roles to different users. These roles are of 2 types, either allows access to a specific role for a specific user or decline access to a specific role for a specific user. MAC assigns security levels to different subjects (users) and objects (relations attribute). There are 4 security levels mentioned according to their priorities:

- TOP SECRET (TS)
- SECRET (S)
- CONFIDENTIAL (C)
- UNCLASSIFIED (U)



MAC can be implemented using Bell-LaPadula (BLP) model or Biba model [2]. In BLP, classification of subject is represented as class(S) and object as class(O) [7]. Bell-LaPadula model implements MAC using 2 properties:

1. A subject S is not allowed read access to an object O unless class(S) >= class(O) [7] .
2. A subject S is not allowed to write an object O unless class(S) <= class(O) [7].

Biba model has similar structure to BLP, but it addresses integrity rather than confidentiality. Objects and users are assigned integrity levels that form partial order similar to that of BLP [4]. The integrity levels in Biba model indicates degrees of trustworthiness or accuracy, which is different from that of BLP model. For example, data stored in C.E.O's machine is given higher integrity level than that of any employee. Following are different levels in integrity: [5]

- Crucial (C)
- Very Important (VI)
- Important (I)

Following are different properties in Biba model: [9]

- Simple integrity: A subject of higher integrity level must not read an object at lower integrity level (No read down)
- Star integrity: A subject of given integrity level must not write to an object of higher integrity level (No write up)
- Invocation property states that a process from below cannot request higher access; only with subjects of lower or equal level.

The first two properties of Biba model is completely opposite to that of BLP model.

1.2 Summary:

Mandatory Access Control policies regulate access to data by subjects on basis of predefined classification of subjects and objects in the system, objects are passive entities storing information such as relations, tuples in a relation or elements in a tuple; whereas subjects are active entities performing data access [6]. The security levels in MAC are top secret (TS), secret (S), confidential (C) and unclassified (U), where top secret is at highest level and unclassified at lowest. It can be represented as TS > S > C >U [7]. There are 2 phases in MAC [2]. First phase is assigning levels of BLP or Biba [2]. Second phase is access enforcement which answers the query " can subject S perform action A on object O [2]. Thus, MAC is an access control in which administrator manages the access control [11]. The usage and access policies defined by the administrator cannot be changed or modified by the end users [11]. The access policy indicates which subjects (users) have access to which objects. MAC has a number of challenging problems and research is done on these problems. The use of MAC as Multilevel Security (MLS) is restricted and is decreasing [8]. MAC contains problems like

- Ambiguous security levels
- Filtration [7]
- Polyinstantization [7]

Here, these problems are associated with Bell-LaPadula model which is used to enforce confidentiality.

2. Problem analysis:

Following are the different problems in MAC:

2.1 Requirement of new security levels:

As stated earlier, in traditional MAC there is no security level for common people (people outside organization) where they can access certain data or information to know organization or business and hence marketing of organization or business is not possible in traditional MAC. Hence, an organization cannot reach apex heights in business by adopting traditional MAC. Hence, an update is required to alter the security levels and include this functionality in my proposed model which is an alternate to MAC.

2.2 Filtration

The security levels are assigned to both subjects and objects. These levels are assigned to values inside each attribute. The Bell-LaPadula model form the basis of MAC [8].The different properties of MAC in Bell-LaPadula model are given as:

Simple security property: Only read down is allowed. A subject can read an object only if its security level is greater than or equal to that of object.

Star security property: Only write up is allowed. A subject can write an object only if its security level is less than or equal to that of object. This is done so that there is no flow of information from higher security level to that of lower one [7].

Eg :- consider a relation employee-

Name	Age	Salary
Stan (C)	19 (S)	20000 (TS)
Chris (U)	20 (TS)	30000 (S)
Morris (C)	26 (C)	25000 (TS)
Stanley (C)	23 (S)	20000 (C)

Appearance of this relation to user (subject) with security level confidential (C)

Name	Age	Salary
Stan (C)	NUL	NUL
Chris (U)	NUL	NUL
Morris (U)	26 (C)	NUL
Stanley (C)	NUL	20000 (C)

The objects which are at higher level than that of subject will be appeared as nul to this subject [7].

2.3 Polyinstantization:

Here, multiple instances of a tuple are created [7]. Consider the above example, the user with security level confidential (C) can view attributes which are at lower level or equal level as compared to this user. Other values are displayed as NUL. These values can be accesses and changed by this user by taking a key which is at lowest level in this relation and any attribute can be accessed using this key or value.

Eg :- The value of Morris's salary which is at top secret level can be accessed and changed by a user at confidential level by using attribute which is at lower or equal security level than user.

Query to change Morris's salary-

```
Update employee
 set Salary=35000
 where Name=Morris;
```

Thus, multiple instances of tuple with name Morris are created.

Name	Age	Salary
Stan (C)	19 (S)	20000(TS)
Chris (U)	20(TS)	30000 (S)
Morris (U)	26 (C)	25000 (TS)
Morris(U)	26 (C)	35000 (C)
Stanley(C)	23 (S)	20000 (C)

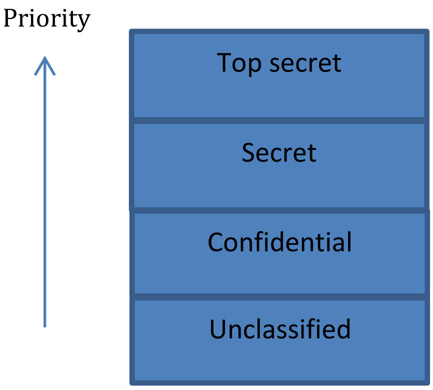
3. Proposed work:

3.1 Proposing new security levels:

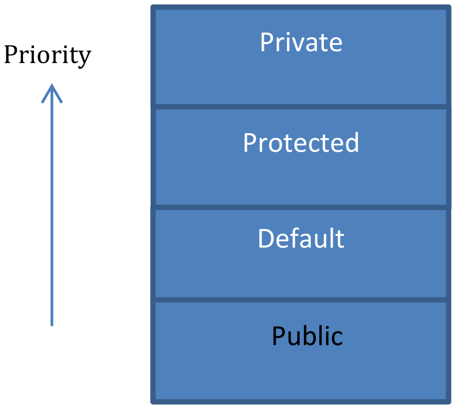
A level which can be accessed by anyone has to be introduced. We can do this by combining java access specifiers with MAC security levels. Thus we get following security levels:

- Private
- Protected
- Default
- Public

Private is at highest level while public is at lowest level. These levels can be assigned to both subject (user) as well as to object (relations). Private is assigned to subjects and objects which are at highest priority and are principal part of an organization which cannot be shared to anyone inside or outside the organization. Protected is assigned to those subjects and objects which are at very high priority and cannot be accessed by those which are at lower level of organization or common people outside the organization. Default is assigned to those which are at lower level of an organization t are a part of organization and information which cannot be shared outside the organization. Public level is assigned to everyone inside or outside this organization. It contains information which can be used to attract new customers or letting know people about your business or organization. Public is most handy level for strategy planners and analysts to advertise your business or organization. Unauthorized person cannot receive any confidential information from accessing public level data or information



Traditional MAC



My proposed MAC

Properties for this proposed model :

Only read down is allowed. A subject can read an object only if its security level is greater than or equal to that of object. Other objects are not provided and cannot be read by that subject

A subject can perform write or modify operation only in that view provided and that also at level which is not less than level of object to prevent flow of information from higher level to lower level. In other words, a subject can only perform write operation if security level of subject is equal to that of object.

3.2 Eliminating filtration:

Here, the security levels are assigned to each attributes instead of values.

Relations

↕

Attributes ⟷ security levels assigned at this step in my proposed model

↕

Values ⟷ security levels assigned at this step in traditional MAC

Eg – considering the above relation employee

Name (Public)	Age (Default)	Salary (Private)
Stan	19	20000
Chris	20	30000
Morris	26	25000
Stanley	23	20000

Appearance of relation at security level Default:

Name (public)	Age (Default)
Stan	19
Chris	20
Morris	26
Stanley	23

Views can be used to hide the objects (attributes) whose security level is greater than security level of subject (user)

3.3 Minimizing polyinstantization:

Since, using views attributes which acts as object are assigned security levels, so problem of filtration is solved. Now, since the attribute which has higher security level is not seen, and then the attacker or unauthorized person will not be able to see that attribute. Hence, it won't be able to trigger the query on that attribute with subject at security level less than that object which reduces polyinstantization. Consider the above example

Appearance of relation at security level Default:

Name (public)	Age (Default)
Stan	19
Chris	20
Morris	26
Stanley	23

Here, the user at default security level does not know that an attribute of private security level exists and hence will not be able to access that attribute through use of lowest level key as it is possible in traditional MAC. But user can access and modify this view of a table provided. It can modify only those objects which are provided in that table. Hence the user at private security level will be able to distinguish easily between original and newly created tuple since some attribute's values are missing in newly created tuple. Then, user at higher level will decide whether to keep that tuple or delete it. The user at higher level can only read tuple or delete it but cannot write anything in order to follow properties mentioned in 3.1.

4. Conclusion:

Thus, we have overcome the drawbacks of traditional MAC. The new security levels can be java access specifiers which are private, protected, default and public. The motivation behind doing this is to let the people outside the organization know about the organization or business and security is also maintained simultaneously. At the same time, by using my proposed model, filtration can be eliminated by going up in hierarchy of assigning security levels. Polyinstantization can also be reduced by enforcing properties stated in 3.1 and through filtration.

The disadvantage of using my proposed model is that users (subject) at higher security level can delete the tuple created by user of lower security level, along with read, and it reflects changes in the database and also to subject at lower security level and can result in flow of information or interest of higher level security to lower level security.

References:

[1] Mandatory Access Control at object level in Java Virtual Machine- Vivek Haldar and Micheal Franz

[2] A General Mandatory Access Control – Fang Yang, Xuihai Zhou and Dalei Hu

[3] Security Fundamentals – Microsoft Official Academic Course

[4] Policy, models and trust - http://cs.brown.edu/cgc/net.secbook/se01/handouts/Ch09-Models.pdf

[5] Biba Integrity Model – Nathan Balon and Ishraq Thabet

[6] Database security- concepts, approaches and challenges –Elisa Bartino, fellow IEEE and Ravi Sandhu, fellow IEEE

[7] Fundamentals of Database Systems Fourth edition – Ramez Elmasri and Shamkant B. Navathe

[8] Multi-purpose implementation of Mandatory Access Control in Relational Database Management Systems – Walid Rjaibi and Paul Bird

[9] https://en.wikipedia.org/wiki/Biba_Model

[10] http://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC

[11] http://www.webopedia.com/TERM/M/Mandatory_Access_Control.html

[12] System and web security – Veer Govardhan Chandar, techmax publications