Journal of Basic and Applied Engineering Research
p-ISSN: 2350-0077; e-ISSN: 2350-0255; Volume 2, Issue 20; October-December, 2015, pp. 1770-1772
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Study of Security Protocols on Access Control

Arijit Choudhuri[1], Debasis Giri[2] and Utpal Roy[3]

[1,3]Department of Computer & System Sciences, Siksha-Bhavana, Visva-Bharati Santiniketan – 731235
[2]Department of Comp. Sc. and Engg. Haldia Institute of Technology, Haldia India-721657
E-mail: [1]arijitc.007@gmail.com, [2]debasis_giri@hotmail.com, [3]roy.utpal@gmail.com

Abstract— *now day's internet is used vastly in commercial purpose and the concept of distributed system has been introduced. Different users or processes on behalf of user are conned to each other for accessing files, resources. To obtained security it is now mandatory to restrict the access to the desired files or resources. Access control mechanism ensures the restriction over accessing different resources. Different access control mechanisms their advantages and disadvantages are discussed in this paper. A mechanism is introduced to overcome the authentication problem to achieve access control.*

Keywords*: DAC; MAC; RABC*

1. INTRODUCTION

Access control terminology was established in the late 1960s by Lampson (1974). Access control is the procedure where the security limiting the activity of users or process on behalf of user. There exists a reference monitor which monitors every attempted access of user or program. The reference monitor then consults with authorization database to validate the user or the program on behalf of user is valid or not. In networked environment it is very difficult to authenticate a proper device. If intruders observe the network traffic then they can break the authentication protocols. Once the authentication is correctly achieved then the access control works properly. There exist three main types of access control policies discretionary, mandatory, role based. In this paper these tree types of protocols and some other protocols which are introduced later on are discussed.

2. DIFFERENT ACCESS CONTROL PROTOCOLS

Lampson's Matrix and Discretionary Access Control

Lampson introduced the formal notions of subjects, objects, and access control matrix. An access control matrix is a easy demonstration in which each entry [a,b] of the matrix specifies the operations or set of operations that can be performed by subject a on resource b. An example from the commercial field is illustrated in Table 1. For example, user A (more accurately processes invoked by user A) is authorized to write and read/access both administrative and commercial records objects and read/access to bills. The matrix is contained with permission list row wise, defining which access is allowed to each user, for example, "D: read access on commercial and administrative records";

Table 1

User	Commercial record	Administrative record	Bills
A	R,W	R	R
B		R	R
C	R,W	R,W	R
D	R	R	

Thus the matrix is contained access control list (ACLs), defining what permissions are granted to the objects, for example, "bills: read access by A, B and C."

These days, an access control matrix is infrequently used with the growing number of resources and users. This model is not suitable for huge organizations. The main goal of new models (e.g., role-based access control) is to conquer these restrictions by proposing organizational grouping of subjects or resources

Discretionary access control (DAC)

A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources.

In previous protocol the matrix has an ownership relation with the subjects to access the objects. It is implemented in the operating systems like Unix/Linux to control access to files (a chown command which changes the owner of a file). This protocol permits granting of permissions to the convenient user. So DAC mechanisms are used widely in commercial purpose but it is also suffer from several problems.

In case of UNIX or Linux operating system user can give any permission to anybody using "chmod 777" command. It is also suffers from transitive access anomaly. That is one user can copy the file from another user and then allow other user to read the content of copied file.

Lattice-Based and Mandatory Access Control

If the user can not able to own the information which they are given permitted access. So mandatory access control is introduced (Bell & LaPadula, 1973). Mandatory access control is based on object classification. Object classification means the objects are classified into different security levels. Administrators can only make change in security levels of object. The higher level is more secured information than lower level. Users can write to higher level classification where as they can only read from lower classification. The permission is given for both read write in same classification. The leveling of user is ensures the authorization of the objects. The MAC protocols is also known as lattice based access control because it is applied on partially ordered levels (combination of several classifications)

Role-Based Access Control

The DAC protocol is not secured and the MAC protocol is too restrictive so RABC is developed. The definition is quoted from Sandhu, Coyne and youman(1996) “A role is a job functions or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role”. Though the different organizations have different hierarchy so assigning the permission is more complex and costly. To overcome this problem RABC is more effective. In RABC rolls can inherit permissions from their parents. Thus the productivity of the system administrator is increased. Here the permissions are given depending upon the roles of the users and users are the members of appropriate roles. RABC is described by four conceptual models. $RABC_0$, $RABC_1$, $RABC_2$, $RABC_3$. The core conceptual model is $RABC_0$, after adding role hierarchy to $RABC_0$, $RABC_1$ is achieved. $RABC_2$ adds static and dynamic constraints between core concepts and $RABC_3$ includes all properties of $RABC_1$ and $RABC_2$. Static constraints means constraints related to session and dynamic constraints means constraints not related to session. RABC is effective for providing large organizations, e-commerce.

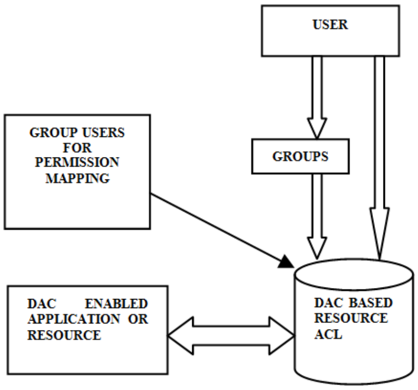
3. COMPARISON

In dictionary access control which subject is accessed by which object is specified by the owner of the object where as mandatory access control based on different security labels. Subjects have security clearance and objects have security classifications (secret, top secret, confidential, etc.). The classification data with clearance are stored into different security labels which are strictly related to specific subjects and objects.

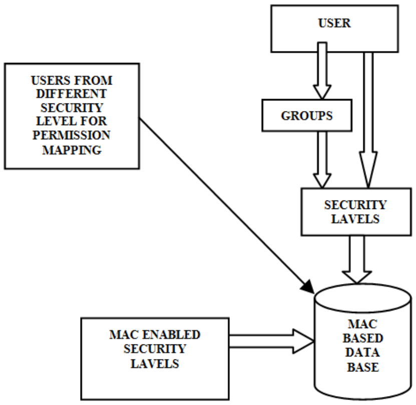
When the system is making an access control decision, it tries to match the clearance of the subject with the classification of the object. For example, if a user has a security clearance of secret, and he requests a data object with a security classification of top secret, then the user will be denied access because his clearance is lower than the classification of the object.

In case of DAC operating systems like windows, UNIX, when one create a file, then he decide what access privileges that he wants to give to other users; when they access the specified file, the operating system will make the access control decision based on the access privileges created by the owner.

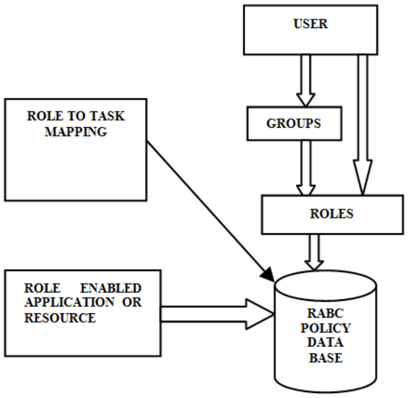
RABC allows individual user to authenticate and access data. It creates roles for the application owners, administrators and assigns privilege to those roles.


USER
GROUP USERS FOR PERMISSION MAPPING
GROUPS
DAC ENABLED APPLICATION OR RESOURCE
DAC BASED RESOURCE ACL

DAC Access control


USER
USERS FROM DIFFERENT SECURITY LEVEL FOR PERMISSION MAPPING
GROUPS
SECURITY LAVELS
MAC ENABLED SECURITY LAVELS
MAC BASED DATA BASE

MAC Access control



RABC Access control

4. PROPOSED METHOD

After going through all the access control protocol it is very clear that all the protocols are based on an authentication technique. The approach is different based on different authentication technique. If we can authenticate proper user or process then all the security aspects of the access control mechanism is maintained. We proposed a method to authenticate the user or process by digital signature. At first the user is verified by the administrator using digital signature. Then after proper verification the access permission is given to that user or the process. Using digital signature we can overcome the problem which is arise in DAC method.

5. CONCLUSION

In the view of security aspects access control is an efficient mechanism for protecting private and confidential information from attackers. Some models are introduced rather than the discussed models which also ensure the confidentiality, integrity and availability. The proposed method is also enhancing the security aspects of access control mechanism. Access control provides a proper protection against cyber terrorist.

REFERENCES

[1] Bell, D. E., & LaPadula, L. J. (1973). Secure computer systems: Mathematical foundations and model. The Mitre Corporation.

[2] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. Computer, (2), 38-47.

[3] Casalino, M. M., & Thion, R. (2013, October). Refactoring multi-layered access control policies through (de) composition. In Network and Service Management (CNSM), 2013 9th International Conference on (pp. 243-250). IEEE.

[4] Belokosztolszki, A., & Eyers, D. (2003). Shielding the OASIS RBAC infrastructure from cyber-terrorism.

[5] Research Directions in Data and Applications Security, 3-14.

[6] Bertino, E., Catania, B., Damiani, M. L., & Perlasca, P. (2005). GEO-RBAC: A spatially aware RBAC. *10th*

[7] Symposium on Access Control Models and Technologies, 29-37.

[8] Biba, K. J. (1977). Integrity considerations for secure computer systems. The Mitre Corporation.

[9] Brewer, D., & Nash, M. (1989). The Chinese wall security policy. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 215-228.

[10] Clark, D. D., & Wilson, D. R. (1987). A comparison of commercial and military computer security policies. IEEE Symposium of Security and Privacy, 184-194.

[11] Department of Defense (DoD) National Computer Security Center. (1985). *Department of Defense trusted computer systems evaluation criteria* (DoD 5200.28-STD).

[12] Ferraiolo, D. F., Chandramouli, R., Ahn, G. J., & Gavrila, S. I. (2003). The role control center: Features

[13] Shiang-Feng Tzeng, Cheng-Chi Lee, and Tzu-Chun Lin. A novel key management scheme for dynamic access control in a hierarchy. International Journal of Network Security, 12(3), 2011.

[14] Debasis Giri, P. D. Srivastava. A Cryptographic Key Assignment Scheme for Access Control in Poset Ordered Hierarchies with Enhanced Security. I. J. Network Security 7(2): 223-234 (2008).

[15] Debasis Giri, P. D. Srivastava. Cryptanalysis and Improvement of Das et al.'s Proxy Signature Scheme. ICIT 2007: 151-154.

[16] R. Mokhtarnameh, S. Ho, and N. Muthuvelu, “An enhanced certificateless authenticated key agreement protocol,” in in Proc. of the 13th International Conference on Advanced Communication Technology (ICACT), 2011, pp. 802–806.

[17] J. Zhang and J. Mao, “An efficient rsa-based certificateless signature scheme,” The Journal of Systems and Software, vol. 85, pp. 638–642, 2012.