Securing Network using Network Access Control, User and Resource Management, and Location-based Security

Darvinder Kaur
Assistant Professor, Department of Computer Science and Technology, Lovely Professional University, Phagwara, Punjab, India

Sonampreet kaur
Department of Computer Science and Technology, Lovely Professional University, Phagwara, Punjab, India

ABSTRACT
The first and primary law of network access control is to limit the access of network resources among the various types of users. NAC basically decides whom to let go onto the network. It decides the validity of user based on their identity and role. But its work does not stop on user authorization. What happens when user gets access to the network resources? This will be described in this paper. In this paper we present a way to secure the network resources using identity-based, role-based and behaviour-based network access control techniques. Resources will be divided into 5 categories and according to the role of user; access to these resources will be defined. These permissions can be changed on the bases of behaviour of the user. This will make NAC dynamic. And for dynamic user management, clusters of user will be formed based on their behaviour. To secure the network location-based security will be used.

General Terms
Network access control, Identity-Based and Role-Based NAC, Behavior-Based NAC.

Keywords
Network Access Control, User and Resource Management, and Location-Based Security.

1. INTRODUCTION
As the number of users on the network increases, so is the need to secure the network resources. Though network resources are for the use of people but sometimes people themselves can misuse resources. To prevent it from happening, one of the ways is Network Access Control. NAC is a technique through which network operator manage the various kind of users. For this purpose, Identity-based authentication mechanism is used to check whether user asking for permission to get onto the network is authenticated or not[9]. But the problem arises when all the users have equal rights to access everything on the network. To solve this problem we will use Role-Based mechanism on the server side, where according to the specified role of user, permissions will be granted[9]. But then it comes to, what type of resources can specific user access-top secret, secret, confidential, restricted and unrestricted information. So network administrator will use the concept of limited privileges.

So, first user will be authenticated, and then according to the user's role permission to specific type of resources will be granted.

But it's all done by network operator/admin, means it's all static in nature. To make it dynamic behaviour-based mechanism and clustering of users will be done. Anytime any change in behaviour of user will be found, his permissions will be changed. User's action and activities will be observed and according to it he will be put into a cluster/group automatically. And, then network admin can assign privileges to that group according to the behaviour of users.

To make user and network more secure location-based mechanism will be used. It will inform the user about hack of its identity based on the location from where he presently accessing the network.

The organization of the rest of the paper is as follows. Section 2 is about various techniques used to control network access; it Include Identity-Based, Role-Based and Location-Based Access Control. Section 3 is about unified Architecture of NAC. Section 4 consists of Conclusion of this paper. Section 5 is dedicated to Acknowledgement.

2. DESCRIPTION OF NETWORK ACCESS CONTROL MECHANISM

2.1 Identity-Based and Role-Based NAC

First, when user asks for permission to access the network, he needs to prove himself as authenticated user. This is done with help of identity-based authentication mechanism. This is done by entering the credentials such as ID and password, by user. Then on server side these credentials are matched with already stored there. If they matched the access to the network is granted otherwise denied. Identity-based is described in Figure1.

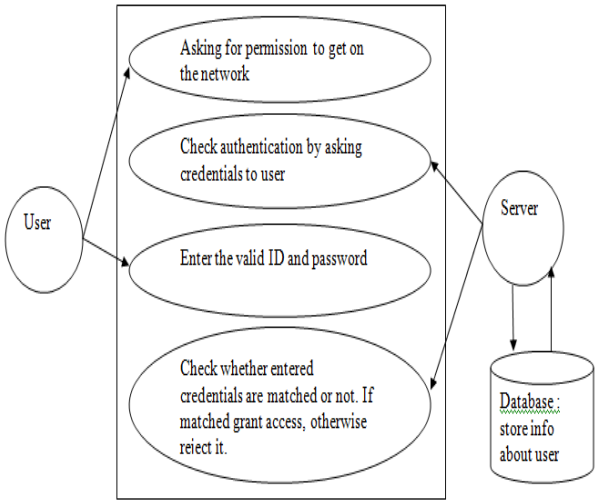

Fig 1: Identity-Based Authentication Mechanism

Once user gets onto the network, he has right to access resources on the network. But not all the stuff on the network is for each and every user. For this purpose concept of Role-Based mechanism is used. Here when users ask for the permission and provide his identity with it, at server side database, his role will also be defined. And according to the Role defined, permissions to access the resources will be defined as well. These permissions are Read, Write, Delete and Modify[6].

For example when a higher level person of management, say CEO (role), of company wants to access the network, first user has to enter unique ID and password, from this server will know who the user is and what will be the permissions. And according to the role (CEO), user will have access to almost all the resources on the network of the company and he can also Read(R), Write(W), Delete(D), and Modify(M) files on the network.

But when a lower level person of management, say regular worker, tries to enter the network, his permissions will be different from the CEO of the company; based on the role, of course. He may only have read and write information but not to modify and delete. So the problem of Confidentiality and Authorization and Authentication is solved. This process this described in Figure 2. According to figure 2, manager can read and write a file on the network and also can edit it but cannot delete it. On other hand regular production worker can only read the files on the network.

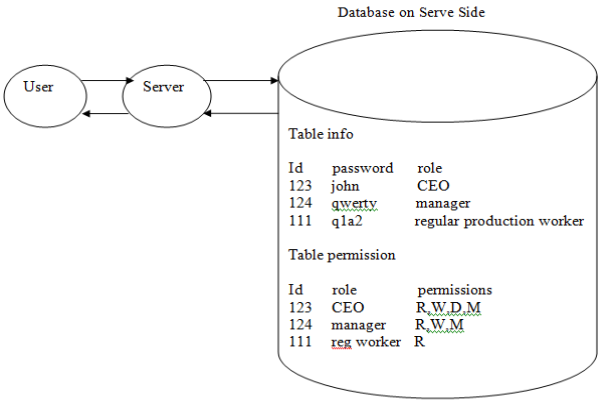

Fig 2: Role-Based Mechanism and Permissions granted to User.

Note: Role-Based Access Control is many to many relations. It means a role can be given to a user and a user can have many roles. Like manager role can be assigned to all the managers in the company and a manager can have two roles like manager and a rag worker

2.2 Resource Management

But one problem is still there, i.e. how much and what type of resources will be seen by whom (acc to role). It means, acc to figure 2, can manager access all the resources on the network and can read, write and modify them. The answer is no. So here is one technique that can be used to eliminate the problem. Network admin can divide the resources into 5 categories i.e. Top Secret (TS), Secret (S), Confidential(C), Restricted(R) And Unrestricted(UR)[9].

Therefore, add one more table to the database, which will tell about the category the specific resource on the network, and who can access them with permissions defined as well. This is described in figure3.

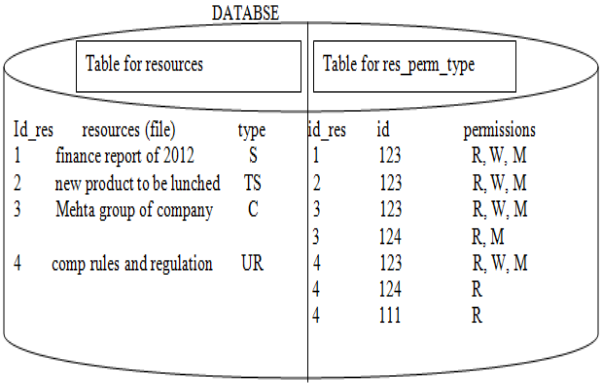

Fig 3: Resource Management by dividing resources into 5 categories

2.3 Behaviour-Based Network Access control

Above all processes need network admin, he has to done things manually. But Behaviour-Based NAC can lighten up the burden on the network admin by making things dynamic. As the name suggest, here permission to access the resources will be based on the behaviour of the user[3]. That does not mean that from the very beginning, when user enters for the first time on the network, permissions will be automatic. No, first, of course, network admin will assign the permissions. But what happens after the access granted to the user is very vital. What type of information user is accessing is user still working acc to the rules and policies defined or not etc. For this purpose we need to observe the behaviour of the user[3].

If the user is not working acc to the policies user's permission will dynamically be changed. Example, say when CEO of the company was modifying the Mehta group company file, at the same time manager also tries to modify. Now this is very critical state. There will be a conflict, what to store and by whom to store. At this very state, permissions of manager will be changed to read (R) only, it means now manager can only read it. But CEO will not be disturbed as he was the first user to access the file. Once CEO has done the modifications and saved it. Then again permissions will be changed to previous once. Now manager can read and modify the file. This is situation is described in figure 4.

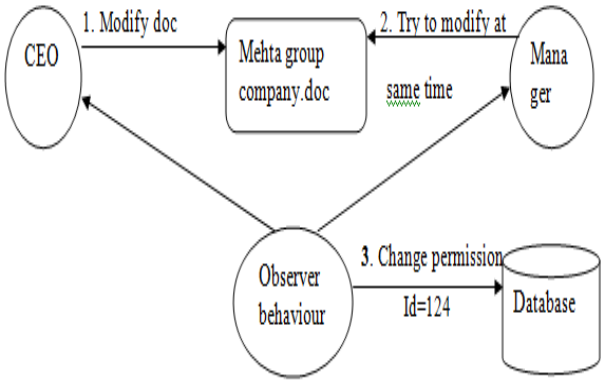

Fig 4: Behaviour-Based Access Control

Behaviour-Based Access Control is done to maintain the consistency in the database and to fulfil the quality of service rule. Let's say so many person are trying to access same

resource on the network at same time, it will affect the performance of the network. If many of them tries to modify it, QoS rule not be fulfilled as everyone will not be able to get updated version of the document[5]. First modification of the file must be done and then it must be avail to other to read.

2.4 Formation of Clusters

The basic law of clustering is to group up the objects with similar nature. And groups are formed so that network admin do not have to grant permission one by one to all the users. Rather he will give same permission to a group once and that permission will automatically will be applied to all the users in it.

Here users will be grouped according to their behaviour and role. Many groups can have any number of users and a user can be in many numbers of groups. This will be done dynamically. First there will be matching of the behaviour and role of the user with the existing user's behaviour and role; if they match new user will get the entry otherwise denied. Like one of the group is for managers only and other is for employees. Now a manager will be in both the groups as he is a manager and also an employee. But a regular worker will only be in employee group. Clustering formation is described in figure 5

Manager group

Id	name	manager
1	Jagman	production manager
2	Gursimren	manufacturing
3	Vibhu	HR manager
4	Neha	transportation manager

Employee group

Id	name	position
1	Jagman	production manager
2	Gursimren	manufacturing
3	Vibhu	HR manager
4	Neha	transportatin manager
5	Harpy	project leader
6	Sukhprit	receptionist
7	Preet	network admin
8	Noor	executive

Fig 5: First group is formed for the managers of the company and other is for the employee in the company.

Now if there one of the resources that are only for the managers for the company then it will only be shared once i.e. to group and every one will have it. And also granting permission will be easy. This all is done dynamically, if the behaviour profile means attributes of user are matched with the given attributes of group then user's ID added to the group. Like here one of the attribute is 'manager' any user having manager attribute will be welcomed in manager_ group.

2.5 Network Access Control for New Users

This also one of the dynamic ways to assign the permissions to users. When an unknown user who does not have profile on network tries to access the network then what to do? For new user everything will be different he will not have access to all the resources on the network. Now network admin will create a group only for new users. All the new users will be put their and they all will have limited access to the network. They cannot modify files on the network and they even will not be allowed to see many of the files, for the sake of confidentiality.

2.6 Location-Based Access Controls

Now this is the new concept of access control. As the name suggest access to network will be based on the location of the user. Basically it is used for the security purposes. Access to the user will be given if the location of the user will be as specified in the server side database. For this, there is need of Global Positioning System (GPS) to find out the current location of the user[1].

Suppose 30 mins ago user has login on the network using correct credentials. And GPS has stored that user was in Jammu and Kashmir. And now again user is trying to get login on the network; user had entered the correct credentials but GPS find out that user is in the Punjab.

This swift change in the location of person will be informed to user by sending him message to user's mobile phone i.e. stored in the database. This is done to ensure about the identity theft problem. If current user is impersonating the real user then real user will have to change the credentials.

Now if at the same time two users are trying to access to the network using same credentials then they will be denied to access the network for some time.

3. UNIFIED ARCHITECTURE OF NETWORK ACCESS CONTROL

To sum up all the above mechanism of network access a unified NAC system can be designed. Network access control does not only mean to deny or allow user to the network but much more. It is the most important step towards security of the network resources as well as security of the user.

This design of NAC is dynamic in nature, more secure, and provide easy user management and resources management [2].

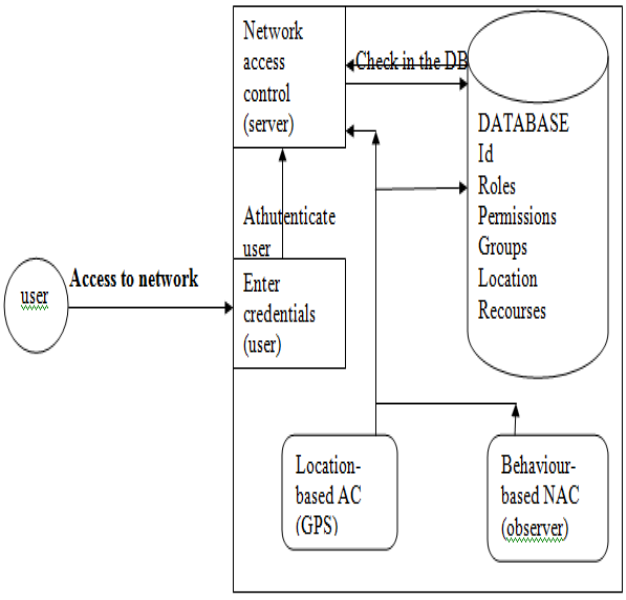

Fig 6: Unified Architechure Of Secure Network

Steps to Network Access Control

1. User tries to access the network by entering the correct id and password.
2. If they are correct; access to the network is given.

3. And also location of the user will be recorded with help of GPS system.
4. If location is correct and matched with the previous one access will be given.
5. And with this observation of user's actions starts
6. If user is acting normal, not breaking any pre defines policies then its ok. Otherwise based on behaviour of user permissions will be changed.
7. Again on basis of behaviour and role of user groups will be formed and according permissions will be granted.

4. CONCLUSION

In this paper we have presented a unified architecture of Network Access Control; that improves network access control and provide dynamic update of permission based on behavior of user. It uses location-based technique to provide user security. Further we will be working on finding out is user fit to access the network before user enters the network. To basically make only secure user to enter the network. If user meets pre-requested policies by network then only user will be granted the access to network.

5. ACKNOWLEDGMENTS

The authors would like to thank everyone who supported points presented here on Network Access Control. This paper is supported by Lovely Professional University, Phagwara, Punjab, India

6. REFERENCES

[1] Lichuin Bao (2008) "Location Authentication Methods for Wireless Network Access Control", International conference on computer engineering and technology

[2] Yabin Liu, Huanguo Zhang , Huanguo Zhang and Bo Zhao(2009) Research on Unified Network Access Control Architecture 2009 IEEE Ninth International Conference on Computer and Information Technology.

[3] Vanessa Frias-Martinez, Joseph Sherrick, Salvatore J. Stolfo, Angelos D. Keromytis(2009)" A Network Access Control Mechanism Based on Behavior Profiles", Annual Computer Security Applications ConferenceTavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Zhen Chen, Fa-Chao Deng, An-An Luo, Xin Jiang, Guo-Dong Li, Run-hua Zhang, Chuang Lin(2010)" Application Level Network Access Control System Based on TNC Architecture for Enterprise Network", Natural Science Foundation of China No. 90718040, National High-Tech Program No.2007 AAO 1 Z468, Hosun Tech.

[5] Shujuan Wang, Mangui Liang (2010)" A Network Access Control Approach for QoS Support based on the AAA Architecture", International Symposium on Intelligence Information Processing and Trusted Computing.

[6] Song, Tiantong You (2010)"A network access control mechanism based on role and behavior", Proceedings of IC-BNMT20 10.

[7] Yanzhe Che, Qiang Yang, Chunming Wu, Lianhang Ma(2010)" BABAC: An access control framework for network virtualization using user behaviors and attributes, IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing

[8] Zhao Jianguang, Liu Jianchen, Fan Jingjing, Di Juxing" The security research of Network Access Control System, 2010 First ACIS International Symposium on Cryptography, and Network Security, Data Mining and Knowledge Discovery,E-Commerce and Its Applications, and Embedded

[9] BAI Qing-hai and ZHENGYing (2011)," Study on the Access Control Model in Information Security", 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference