THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Management of Data Security in Distributed System

Harvendra Singh
M. Tech (ISM) 2nd Year, Dehradun Institute of Technology
Dehradun, Uttrakhand, India
Anuj Yadav
Assistant Professor, Department of Computer Science
Dehradun Institute of Technology, Dehradun, Uttrakhand, India

Abstract:
This approach deals with management of data security in client/server system and distributed system. In this paper, we present how to manage the data security in system, examining their vulnerable points and discuss their solutions. And, we also describe the main component of data security management of distributed system- Authorization, Authentication, Encryption and Access control. With an analysis of the management of data security, we will also present an access security system based on client/server architecture, which included with security services. This model describes the access security server and interface for access security which is combined with application and portion of client. Nowadays, security is main issue but the main importance is how to manage these security issues. More ever, in view of increasing importance of security and usually use of data security management technology, this approach is importance for the theoretical and applicative point of view.

1. Introduction

The protection of data should be big issue for every organization, for the organization's ability to survive depends on availability, comprehensiveness of its financial and organizational data. Security has more complicated with increasing use of personal computer's networking. At this time, connection between small and big computers and local networks are parts of them which takes part in the application. So the data is not fully protected on the network and unauthorized user can access the data using different types of tools. From prevention of data from unauthorized access, we require coordination and management of data security. Unfortunately, many organizations do not deal with security issues until fault is not occurred in the network.

To prevent the vital data of organization, organization must set up a security system before the attack is occurred. Also, this includes risk identification, use sufficient means of security and learn to users about security awareness.

1.1. Distributed System

Distributed system is a collection of independent, networked, communicating and physically separate computational nodes. The most important part of distributed system is its joint data network which is the centre of the organization. Distributed systems have following characteristics:

- Multiple autonomous components.
- Resources may not be accessible.
- Multiple points of control.
- Multiple points of failure.

1.2. Client/server System

In earlier days, traditional distributed system enable users to use data and applications on distant networks without knowing them to networks that they are directly connected to. Clint/server applications are very flexible and allow users to access database on different networks via graphical interface. In client/server system, the functionality of mainframe is divided into two parts:

- Client: A user interface
- Server: Management of database on another system.

1.3. Components of Security System in Distributed System

There are four main security components: Security authorization, authentication, encryption and access control.

- Authorization: Authorization is the process of giving someone permission to do or have something and is also the process of granting or denying access to a network resource. The authorization is examined by software servers which have all information about users like user name, password etc.

- Authentication: Authentication is any process by which you verify that someone is who they claim they are. Authentication is realized by a hardware device like pocket computer or credit card that creates a password and transfers it to the authentication server that is connected to the networks.
- Access control: Access control is the act of ensuring that an authenticated user accesses only what they are authorized to and no more. It is implemented by access matrices, access lists etc.
- Encryption: Encryption is the process of encoding message and information in that way that only authorized users can read it. It I implemented using algorithm such as DES, RSA, AES etc.

1.4. Security aspects of Client/server System

The distribution of services in client/server increases the susceptibility of these systems to damage from viruses, frauds, physical damage and misuse than in any centralized computer system. It is possible to point out the following threats in client/server systems.

- The work station may be installed in high risk area.
- The work stations approval mechanism of the users may be partial.
- Possible to carry out automation of the login procedure.

2. An Access Security Model

In this part of the paper, we will represent a model in a local area network (LAN) with many stations and users. The aim of this model is incorporated access security mechanism which will authorize the users and supply the password to the stations of the network. This model is suitable for systems in which the operators use a large number of queries and transactions like updating, inserting and modifying. Now explain with an example of data system at any branch of bank. The system includes a large numbers of queries and many transactions which is activated by clerks according to various departments. According to hierarchy of the branch- manager, deputy manager, department managers, clerks- Sectionalization of transactions and users take place. A clerk of the current account department will do only current account transaction not other.

This model defines two main characteristics: authority and authorization. Authorization is the process of giving someone permission to do or have something. Authority is the functionality level of the user in organization. For example, in a branch highest authority is the manager and then department manager and so on.

2.1. Architecture of Model

This model is based on Client/server architecture in described in figure. This architecture may operate at each of the stations. The various clients will receive the access security services via an interface where these services are required. In this model we will use PIPE which is communication mechanism between the client and server. This method is used for passing information from one computer process to another process with a specific name. A named pipe can be used by processes that do not have to share a common origin. The message sent to named pipe can be read only by authorized user that knows the name of the pipe. The most feature of the named pipe is that it works only using "FIFO" method means first in first out.

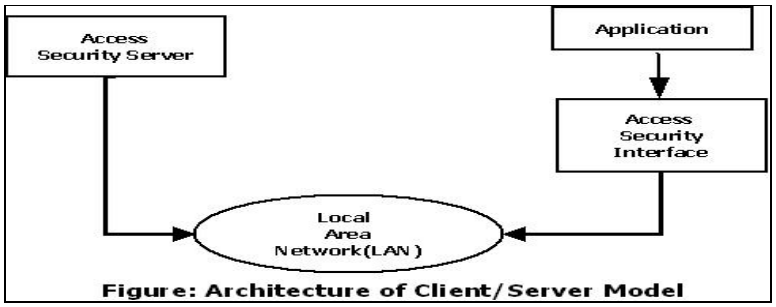

Figure 1

3. Characteristics of Access Security in System

This system refers to users carrying out a number of transactions at their work stations. The proposed access security system will provide a number of services for the client's application which will enable a good access security level. There are also create a backup of each server and the series of the services applied to both client and server. The following are specifications of the access security services:

3.1. Transactions

- Define a new transaction
- Delete the existing transaction
- Update the transaction details
- Receive the list of transactions authority
- Receive authority for transaction

3.2. Stations

- Add a new station
- Delete the existing transaction
- Update the details of station

3.3. Employees

- Define a new employee
- Delete the existing employee
- Update the details of employee
- Examine the validity of employee
- Examine the password of employee
- Receive authority of employee
- Change the password
- Check the blocked employee
- Receive the list of authorized employee

3.4. Additional Services

- Examine the validity of password
- Primary password
- Registration of transaction

4. Application of Layered Design in Data Security

In a layered design, it is possible to dismantle the complicated programs. Each layer has a service interface. This layered system also organized the communication between two independent programs. Communication between two programs may be identical in each program. There are following three principles of this layered system:

- Both the layer on client and server side together provide services. This protocol specifies how the work is divided, message format and order of transactions.
- At the higher level, the service is simple.
- The service interface defines how each layer requests and receives the services of the layer also the interface must hide all the details of transaction.

Now, we discuss the layered system in Client/Server model. The server can store data in a large scale like as documents, records, videos etc. This model divides the client/server programs into three layers: the application layer, the talk layer and the communication layer.

- **The Application layer:** On the client side, the application layer is the program requiring data services, activating them with calling the service function in the higher level. On the server side, this layer carried out the client's request, approach the file, check the user's authorization, also carried out the password, change of password etc.
- **The Talk layer:** On the client side, the layer constructs the message to server and it includes relevant data which is required. On the server side, this layer analyzes the requests sent by the client, identify the kind of service requested, make the proper parameter for transaction and then return to the layer what is required to carry out the transaction. Otherwise this layer also sent the rejection message to the user.
- **The Communication layer:** On the client side, transfer of data is carried out between two processes. In this layer, Named pipe is used if the process on the same computer. If both client and server are on different computers then the communication is carried out at any of protocols of OS/2 which is based on LAN. This layer applied as a generic layer so that we can use the named pipe, Netbios, TCP/IP. The transfer of data over the LAN is transparent.

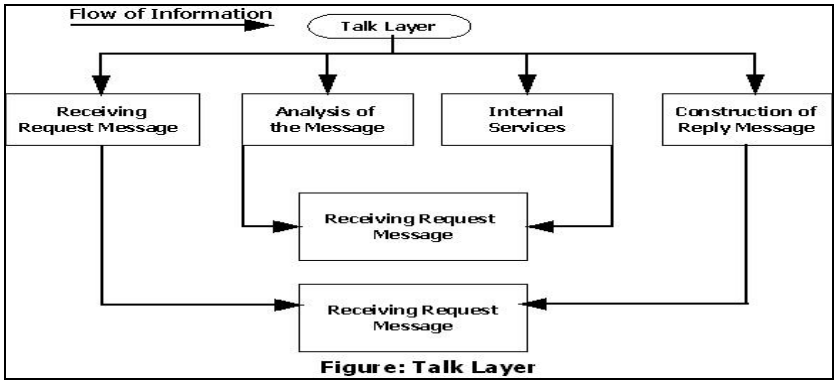

Figure 2

5. Conclusion

In this paper, we developed a security model with client/server application. This concerns many organizations have for protecting their data and applications from intruders in a large numbers of users in environment, can be eliminated. A new way to do is through the implementation of an access security model. The various models for data access security in a distributed system have not provided an effective and comprehensive solution dealing with all aspects of computerized system. This model also seems to answer all four security components: Authentication, Authorization, Access Control and Encryption. The services are given by this model appeal now more than ever due to the increasing importance of this security management technology. This model is useful for those managers who have many stations and users for authorized the users and stations of the network, supply the passwords on the local area network.

6. References

1. Data Security Management In Distributed Computer Systems, Adi Armoni, Tel-Aviv University, Israel, Data Security in 2002.
2. Burleson, D. (1998), Managing Security in a distributed database environment, DBMS, 8, pp. 72-77
3. Harold, J.H. (1998), Random bits and bytes, The Internet and Computer Security, Computers & Security, 13.
4. Neuman, D. (1998), Firewall Follow-up, Data Communication, March 1998