A New Approaches to Improve Server Secuirty by Using Media Access Control Address Verification

[1]Ako Muhammad Abdullah , [2]Miran Hikmat Mohammed Baban , [3] Roza Hikmat Hama Aziz

[1,3]Computer Science Department, Faculty of Physical & Basic Education , Sulaimani University, Kurdistan Region-Iraq
[2]Computer Science , Faculty of Science, Sulaimani University, Kurdistan Region-Iraq

***Abstract*— A Local Area Network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Currently, LAN has been widely used in the different fields. Depending on the requirements of an organization and the kinds of technology used, a LAN can be extended throughout a company or institutions and include voice, images, texts, and videos peripherals. Security in a local area network comprises of the provisions and policies adopted by a network administrator to monitor and prevent unauthorized access, modification, misuse or denial of a computer network and network accessible resources. Network security covers a variety of computer networks, both private and public, that are utilized in everyday job conducting transactions and communications among government agencies, individuals and business. Network can be private, such as within an institutions and company. The most common and simple way of protecting a network resource on server is by assigning a unique name and corresponding password for clients to access a server to get information. In this paper, we propose a new approach to improve server security in a local area network by checking MAC address when the clients want to access the server. The system has been designed to deal with low security level on the server. To do that different testing has been implemented on the system to identify the improving security on the server. The experiments result show that the new security method is efficiency and accuracy in improving the security on the server and the method can effectively deal with clients to access the server in a local area network.**

Keywords— *Local Area Network, Server, Media Access Control Address (MAC Address), Common Gateway Interface, Database Server, Authentication.*

I. INTRODUCTION

The local Area Network (LAN) is a technology that has evolved to meet the needs of automating short distance communication at high speeds of operation, relatively low error rates and providing services and applications to people within a common organizational structure, such as campus, region or a single business. A LAN can be administered by a single organization. On the network, the administrative has the ability to control and governs the security and access control policies. Nowadays, LAN is a useful technology to sharing of expensive resources and high speed mass storage devices among many users is a direct economic benefit to management equate to significant saving. In educational field realize the importance of local area networks in their daily activities and recognize that networking is desirable for optimum educational effectiveness [1].

In order to design and build a well secured on the local area network, many factors must be taken into consideration, such as the topology and placement of hosts within the network, the selection of hardware and software technologies and the careful configuration of each component [2]. Furthermore, the security requirements of the network have changed. The security and privacy expectations that results from the use of LAN to exchange confidential and business critical information exceed what the current architecture can deliver. With rapidly expansion communication, the network architecture is needed to embed security to protecting the information within the packets transmitting over the network and the information stored on the network attached devices and a system designer have to limit the types of interactions that a given user can have with the entire system and accessing the users to the server [3]. Network security issues include protecting data from unauthorized access and viruses. For a network to be useful, sensitive data must be protected from unauthorized access. Protection can be accomplished at a number of levels. At the lowest level are user identification codes and passwords. At a higher level are encryption techniques [4] when transmitting information occurs over the network.

The content information of the individual packets is not readily known to the devices and facilities through which the packets travel. To protect the content of individual messages many tools and procedures are being implemented to provide the security for the content because the interpretation and reassembly of the content is delegated to programs running on the individual source and destination [5].

In this study, a new approach is proposed to improve a security on the server of Local Area Network when a client wants to communicate with the server. This research is to examine the security issues commonly found in the small to medium sized LAN set up for a business or other institution, and to identify the best practices from the perspective of the

network designer. This proposed is implemented by using client Media Access Control Address (MAC Address). The rest of this research is organized as follows: Section 2 presents the background and literature review, Section 3 presents the description of the design and implementation, Section 4 presents the experimental environment. . In Section 5 the results of the investigations are presented and discussed. The final Section presents conclusions and future work.

II. BACKGROUND AND LITERATURE REVIEW

A. *Media Access Control Address*

One of the most important aspects in every networking system, Local Area Network is using the concept of MAC address because it is the one of the network layers (Layer 2) which works on showing the network details on LAN. Also, this address is known as "data link layer" which used to identify hardware on the network. Furthermore, network administrator on the server can be ensured with every client that have fully permissions or unpermitted through their MAC address [6][7].

Beside MAC address there is another aspect which is IP, also known as Network Layer (Layer 3), which is used to connect computers to the network within IP range. Every computer, on local area network will be assigned with a permitted IPv4 or IPv6, 32bits, 64bits in order [7].

B. *Client Authentication*

Nowadays, as technologies have been developed dramatically, lots of hackers, intruders and attackers made a big threaten all over the world. Thus, a concept of network security becomes a big factor between technical and programmer's people to think about proposing a new method to protecting their system from them. So a login system came into account between servers and systems which work on identify the permitted user from disallowed clients, through using username and passwords. This technique can protect users details to be accessed by other people [8].

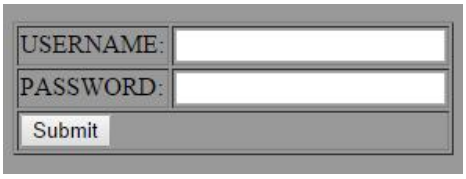

Fig.1 Client Authentication

C. *Server Authentication*

In addition to client side authentication there is another authentication which can be provided by the servers which is permitted MAC address. This technique works on registering allowed client MAC address into the database server. This will prevent any other MAC addresses which are not registered on the local area network. Therefore we can provide a second level of security which helps the system to get consistency and security [9].

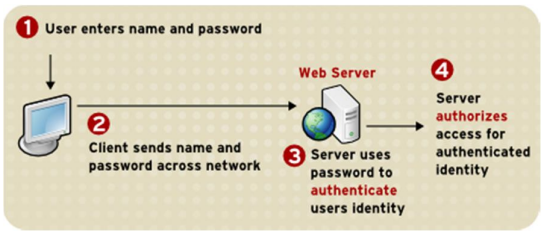

Fig. 2 Server Authentication

D. *Common Gateway Interface (CGI)*

The World Wide Web (WWW) becomes a common subject between users and internet. In addition, all web servers in the world such as apache server and IIS which work on manipulate the web pages and data that requested by internet users into the servers. However, CGI is the main part in the server holds information for users when they requested from them for instance images, text, videos and sounds. Moreover, any form that can be run at any server the CGI is the main responsible to process the content the form with the database server [15].

III. DESIGN AND IMPLEMENTATION

The design phase focuses on the detailed implementation of the system. The design phase is a transition from a user-oriented document to a document oriented to the programmers or database personnel. System design is a process through which requirements are translated into a representation of system. Initially the representation depicts a holistic view of system. Subsequent refinement leads to a design representation that is very close to source code. Design is a place where quality fostered in system development. Design provides us with representations of system that can be assessed for quality; this is the only way that can accurately translate the user requirements into finished system. System design serves as the foundation for all system and maintenance steps that follow. System design goes through two phases of development: logical and physical design [13].

In addition, implementation is the stage in the system where the theoretical design is turned into a working system and is giving confidence on the new system for the users that it will work efficiently and effectively. It involves careful planning, investigation of the current system and its constraints on implementation, design of methods to achieve the changeover, an evaluation, of change over methods. Apart from planning major task of preparing the implementation are education and training of users. The more complex system being implemented, the more involved will be the system analysis and the design effort required just for implementation.

An implementation co-ordination committee based on policies of individual organization has been appointed. The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out, discussions are made regarding the equipment and resources and the additional equipment has to be acquired to implement the new system.

Implementation is the final and important phase. This is the most critical stage in achieving a successful new system and in giving the users confidence that the new system will work is effective. The system can be implemented only after thorough testing. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain type of transactions while using the new system [14].

In our work we planned to design a secure way for clients in order to recognize between permitted and unpermitted users of server. We have done this by using MAC address, which has been used to reject any clients to be used on server which has not been registered before.

On every first process users need to get a GUI for login system, this will be the first step in the system that users use to enter into the server. To make this process, it will need that users must have their own username and password, also their MAC address should be registered before. With this process we came into two different cases, firstly if the user has entered wrong username and password they need to reenter them in correct way.

Furthermore, users must have their MAC address registered into the server; otherwise there will be terminated directly. However, on the accepted case, they will be directed to the "welcome page", and they will have full access to the system, and they can use their features.

To show our work in more details, we created a flow chart as shown in fig-5:

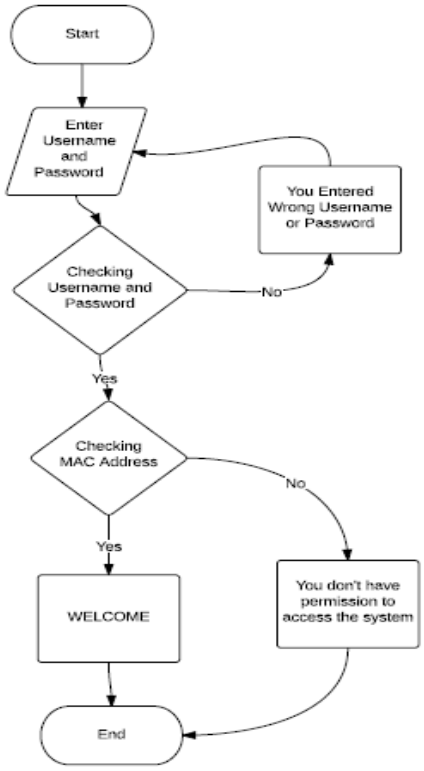

Fig. 3 Flow Chart of Server Security Verification

IV. SYSTEM TESTING

The completion of a system is achieved only after it has been thoroughly tested and implemented. Though this gives a feel the system is completed, there cannot be any system without going through this stage. Though the programmer may take many precautions not to commit any mistakes that crop up during the execution stage. Hence in this stage it is decided whether the system can undergo the real time environment execution without any breakdowns, therefore a package can be rejected even this stage. In short this stage is meant to decide if the package is good for complete implementation [10].

A. Testing Methods

Testing is a set of activities that can be planned in advance and conducted systematically. The proposed system is tested in parallel with the software that consists of its own phases of analysis, implementation, testing and maintenance [11]. Following are the tests conducted on the system.

1) Unit Testing

During the implementation of the system each module of the system was tested separately to uncover errors within its boundaries. User interface was used as a guide in the process.

2) Functionality Testing

To determine if the various display screens meet the design rules and functionality are complete and correct.

B. Acceptance Testing

Acceptance testing is done to verify for implementation and use. The proposed system provides the end-user confidence and ensures that the software is already to use. Furthermore, the performance of the system is evaluated, and has found that the system works accurately and efficiently in a local area network [12].

V. RESULTS AND DISCUSSIONS

In our propose system, we have tested our work on 21 clients in a local area network which has been joined with a server. The administrator of the system has the ability to create a username, password and registering client MAC address on the server. The users can login through the client computers in the local area network with their username, password and MAC address. Furthermore, our proposed system allows only registered users in a database server to access the server. We have got the following results:

A. Denied Client Access

This case show that the client cannot access to the server due to the MAC address for the client is not available in the database server as shown in the Fig. 1

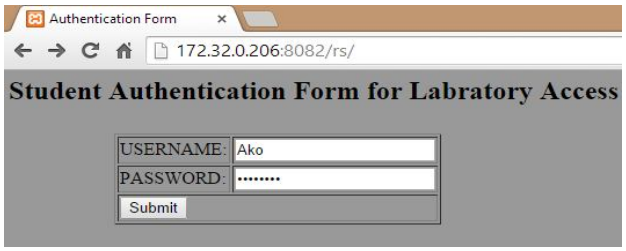

Fig. 4 Login Interface

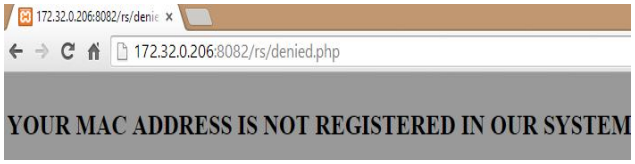

Fig. 5 Denied Client Access

B. Incorrect UserName or Password

The client tried to access the server with unpermitted username or password. However, the client's MAC address is registered into the system thus it cannot reach the system as it can be seen in Fig. 2

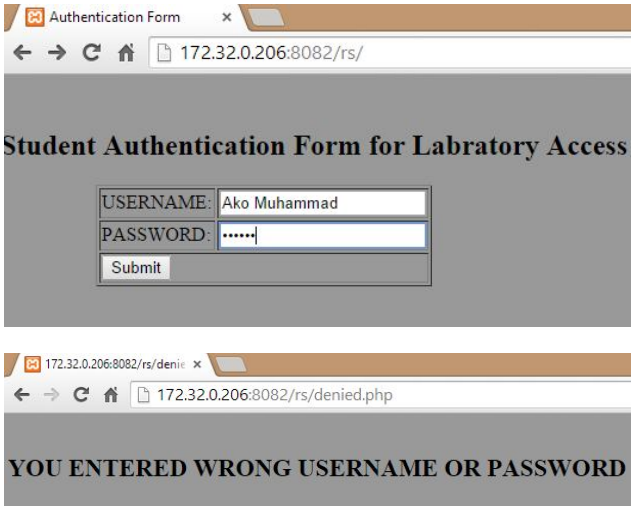

Fig.6 Incorrect UserName or Password

C. Full Permitted Clients

This page means that the users accessed the server with validate username, password and permitted MAC address therefore clients have full permission to use the system. In Fig. 3 presents the full permissions clients.

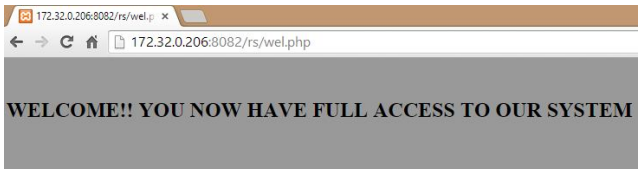

Fig. 7 Full Permitted Clients Access to Use the System

In all results- during testing this system we can observe that the server has fully denied all clients whom their MAC addresses are not recognized by the server. On the other hand, it has allowed all clients who are entered the correct username and password with permitted MAC address. Furthermore, the system is not allowed any clients who are entered the wrong username and password even they have permitted MAC address. The administrator with minimum knowledge can be able to operate the system easily also this new approach has been provided to help the administrator to take necessary, correct action while using the system in a local area network. To implement accuracy of data in all formats of input many validation techniques have been used. This system can be used by any institute and company as it can be modified easily; additional features can be added without interrupting the normal functioning of the system.

VI. CONCLUSIONS

System security is an important aspect in a network. The servers on a local area network have to ensure the facility of preventing unauthorized users from accessing the information and data within the server. The system security must be provided total protection for each user's information so that the integrity of data is sustained and also prevent the system from hacking by intruders. The aimed of this research is proposed a new approach system to improve a server security on the local area network by providing a username and password login for each authorized users with registering their MAC address in a database on the server. Our approach starts with the welcome page prompting the user to establish his/her authentication after that user can access the server. To sum up, we found a good way to improve a security level for accessing database servers from clients through using AMC address to distinguish between permitted users and unauthorized clients. Also, this idea will help each user to keep their sensitive data to be in secure mode.

In the future work, we will try to implement our system on Linux serves with using mobile application, which user can use their smart phones for accessing the server.

ACKNOWLEDGMENT

A big thanks like to be given to University of Sulaimani by authors for their helps and supports in the implementation in our research.

REFERENCES

[1] Espiritu, R., *Local Area Network (LAN) Compatibility Issues*, Thesis, Naval Postgraduate School, United State, 2011.

[2] Dye, M., McDonald, R. and Rufi, A., *Network fundamentals*, 1st ed. Indianapolis, Ind.: Cisco Press, 2008.

[3] Forouzan, B., Coombs, C. and Fegan, S., *Data communications and networking*. 1st ed. Boston: McGraw-Hill, 2001.

[4] Vacca, J., *Network and system security*, 1st ed. Amsterdam: Syngress, 2014.

[5] Franklin, M., Crowley, P., Hadimioglu, H. and Onufryk, P., *Network Processor Design*. 1st ed. Burlington: Elsevier, 2002.

[6] Singh, G., Security Issues in Wireless Local Area Networks (WLAN), *Global Journal of Science Frontier Research Mathematics and Decision Sciences*, Vol. 12, Issue 11, pp.1-12, 2012.

[7] Archana, H. and Gauri, V., Media Access Control Spoofing Techniques and its Counter Measures, *International Journal of Scientific & Engineering Research*, Vol. 2, Issue 6, pp.1-5, 2012.

[8] Fu, K., Sit, E., Smith, K. and Feamster, N., The Dos and Don'ts of Client Authentication on the Web, *in Proceedings of the 10th USENIX Security Symposium. Washington, D.C.*, pp.251--268., 2001.

[9] Hess, A., Jacobson, J., Mills, H., Wamsley, R., Seamons, K. and Smith, B., Advanced Client/Server Authentication in TLS, Computer Science Department, Brigham Young University, pp. 1-12, 2002.

[10] Nguyen, H. (2001), Testing applications on the Web, 1st ed. New York: Wiley.

[11] Manju, K. (2014), Human Resource Management Systems HRMS, [Online] Scribd.com. Available at: http://www.scribd.com/doc/53922861/Human-Resource-Management-Systems-HRMS [Accessed 15 Jun. 2014].

[12] Shakya, H., Report of Online Banking System, *Department of Information & Technology, Pajasthan Technical University, India*, pp.1-70, 2012.

[13] Kumar, V. (2012), Implementation of Eccentric Network for Intranet, [Online] Scribd.com. Available at: http://www.scribd.com/doc/118093298/Eccentric-Network-for-Intrnet [Accessed 12 May. 2014].

[14] Ramesh, K., Babu. B and Prakash, G. ,Scalable Technique of Cryptographic Key in Supervision for Essential to the Success of Wireless Improvised Networks, *International Journal of Engineering Research and Development*, Vol. 5, Issue 2, pp. 14-19, 2012.

[15] Odagiri, K., Shimizu, S., Ishii, N. and Takizawa, M., Principle of Virtual Use Method in Common Gateway Interface Program on the DACS Scheme, *International Journal of Computer Networks & Communications (IJCNC)* Vol.4, No.1, pp.147-161 ,2012.