IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 6, Dec-Jan, 2015
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Network Security Using Multiserver Authentication

Mr. Yogesh R. Bhuyar[1], Dr. G. R. Bamnote[2]

[1]Research student, Information Technology P.R.M.I.T&R.(Badnera), Amravati, Maharashtra, India

[2]H.O.D. , Computer Science & Engineering Department, P.R.M.I.T&R.(Badnera), Amravati , Maharashtra, India

Abstract

In this paper, we propose multi server authentication system with user protection in network security. We first propose a single-server system and then apply this technique to a multi-server system. Addition to user authentication and key distribution, it is very useful for providing privacy for users. The key factors include. The privacy of users can be secured. A user can freely choose his own password. The computation and communication cost is very low. Servers and users can authenticate each other.

Keywords: *Network security, privacy protection, Heartbeat, user authentication Time to leave (TTL) .*

1. Introduction

In order to use services securely in a network and providing security to the data in this paper we provide high levels of security by using multiserver authentication every level has its own security and the user have to get authenticate the levels in order to access the secure data. In this paper we use three ways of authentication scheme first user login through user name and password which is been check in the database if it matches with the database then user precede to the next level Only passing a password for authenticating between the user and the server is not sufficient, since it contain less amount safety and is easily hack by the intruders. Before two parties can do secure communication, a session key is required for protecting subsequence communications. Also, using smart cards, remote user authentication and tokens are generated which contains client ip,server ip,client id,login time and time to leave. Security against proxy .In the first level of authentication is use to detect if the login request is coming via proxy server.

Security against controlled time access. In this case the user login and a ticket is given to the user the ticket contains Client ip, Server ip, Client id, Login time, TTL (Time to leave) Security with Heart Beat. While sign up the Heart Beat of the user is save in the database So while login we record the Heart Beat is check in the database and is compared with the save pattern in the database.Password authentication scheme at both the point of the communication. Since then, many technique have been proposed to point out its drawback and improve the security and efficiency of Lamport's scheme.[3] Only passing a password for authenticating between the user and the server is not sufficient, since it contain less amount safety and is easily hack by the intruders. Before two parties can do secure communication, a session key is required for protecting subsequence communications. Also, using smart cards, remote user authentication and key agreement can be simplified, flexible and efficient for creating a secure distributed computers environment. It is also useful for providing identity privacy for the users.

2. First Level of Authentication

In first level of authentication security against proxy server is check. In this level of authentication is used to detect if the login request is coming via proxy server. Suppose user click on login at 3.10 pm the and sends the login request at 3.15 pm and login request process at 3.18pm then there is a chance that request might come from proxy server. The user login id and password are check in the database if the login id and password are match with the database then user proceeds to the next level of authentication.

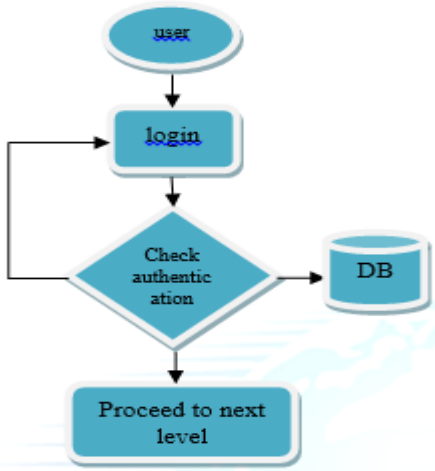

Fig. 1 first level of authentication.

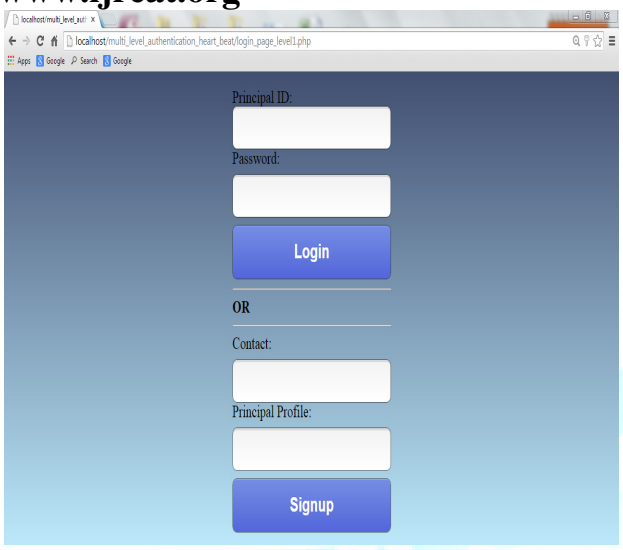

Fig. 2 Login page.

3. Second Level of Authentication

Security against controlled time access. In this case the user login and ticket is given to the users. The ticket contain s. Client ip, Server ip, Client id Login time ,TTL (time to leave). Suppose the current time is 3.18 and the login time is 3.15 and the TTL is 300seconds. Then current time –log time.ie 3 minutes=180 seconds. This is less than the TTL. So user is login. If the current time –Login time =600seconds which is more than the 300 seconds therefore the user is logout.

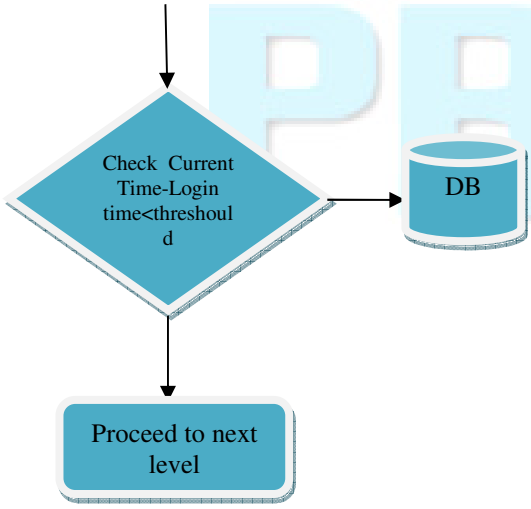

Fig. 3 Second level of authentication.

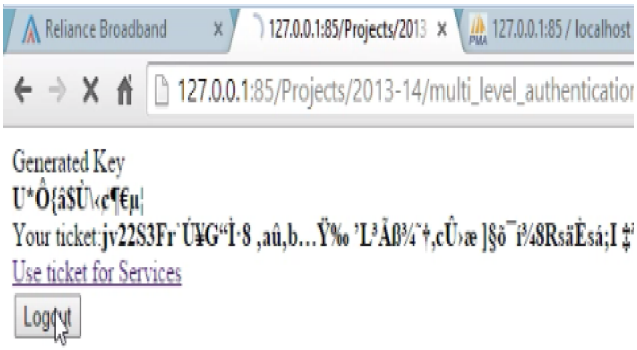

Fig. 4 Token generated.

The ticket generated contain client ip, server ip, client id, login time, TTL (time to leave) which check the threshold value .

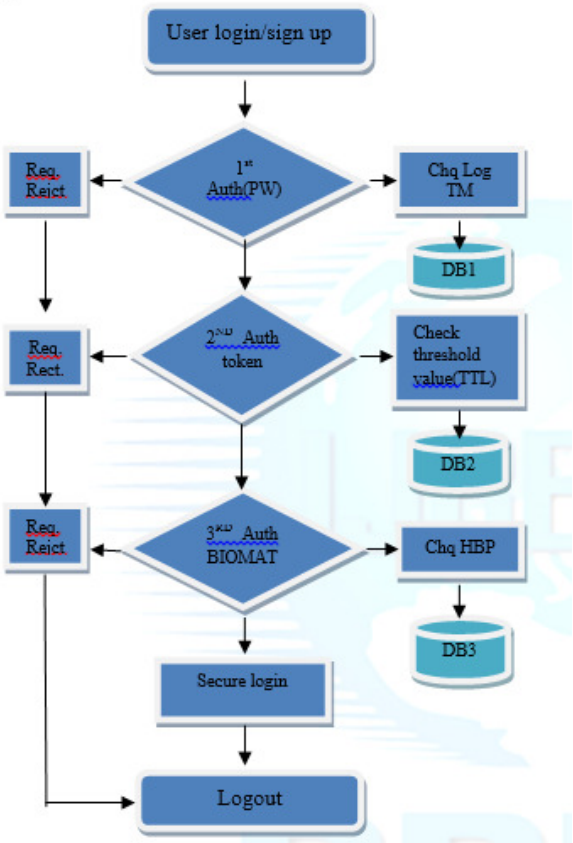

Fig. 5 Multiserver Authentications.

4. Three way Authentication

Security with Heart Beat while sign up the heart beat of the user is saved in the database. So while login we record the Heart Beat of the user and compare it with save pattern to find the difference or variance. If variance is less than threshold than the user is login else logout.

The security tokens generated contains client ip, client id, server ip, login time, TTL. (Time to leave) If the current ip address and the client ip matches with the ip address in the ticket it is suppose that user is not under attack but if the current ip and ip present in the ticket generated does not match the user is logout.

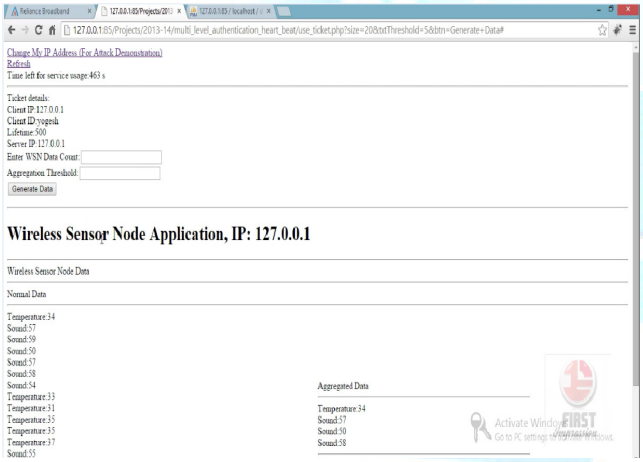

Fig. 6 Results of Multiserver Authentication System

5. Heartbeat Measurement

Heart rate measurement indicates the soundness of the human cardiovascular system. This project demonstrates a technique to measure the heart rate by sensing the change in blood volume in a finger artery while the heart is pumping the blood. It consists of an infrared LED that transmits an IR signal through the fingertip of the subject, a part of which is reflected by the blood cells. The reflected signal is detected by a photo diode sensor. The changing blood volume with heartbeat results in a train of pulses at the output of the photo diode, the magnitude of which is too small to be detected directly by a microcontroller. Therefore, a two-stage high gain, active low pass filter is designed using two Operational Amplifiers (OpAmps) to filter and amplify the signal to appropriate voltage level so that the pulses can be counted by a microcontroller. The heart rate is displayed on a 3 digit seven segment display.

Heart rate is the number of heartbeats per unit of time and is usually expressed in beats per minute (bpm). In adults, a normal heart beats about 60 to 100 times a minute during resting condition. The resting heart rate is directly related to the health and fitness of a person and hence is important to know. You can measure heart rate at any spot on the body where you can feel a pulse with your fingers. The most common places are wrist and neck. You can count the number of pulses within a certain interval (say 15 sec), and easily determine the heart rate in bpm.

6. Conclusions

In this paper we have presented authentication using multiserver in order to obtain data securely to avoid any attack on it various levels of authentication is begin use in order to apply authentication process to various server. Regarding the multi-server scheme, users only need to register one time and can use all provided services by service providers. Both our proposed schemes have the ability of privacy protection.

References

[1] M. Alzomai , " Identity Management : Strengthening One Time Password Authentication Through Usability ". PhD thesis May 2011.

[2] H.C. Kim, H.W. Lee, K.S.Lee , M.S. Jun, " Design of One-Time Password Mechanism using Public Key Infrastructure ".978-0-7695-3322-3/08 © 2008 IEEE DOI 10.1109/NCM.2008.77.

[3] J.L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table", Computers & Security, Vol. 27, No. 3-4, pp. 115-121, May-June 2008.

[4] Y.P. Liao, S.S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standards & Interfaces, Vol. 31,

[5] S. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.

[6] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, 1990.

[7] Y. Chang and C. Chang, "Authentication schemes with no verification table," Applied Mathematics and Computation, vol. 167, pp. 820-832, 2005.

[8] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.

[9] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," Computers & Security, vol. 24, pp. 619-628, 2005.
[10] M. Hwang, C. Lee, and Y. Tang, "A simple remote user authentication ," Mathematical and Computer Modeling, vol. 36, pp. 103-107, 2002.
[11] T. Hwang and W. Ku, "Repairable key distribution protocols for internet environments," IEEE Transactions on Communications, vol. 43, no. 5, pp. 1947-1950, 1995.