Volume 3, Issue 4, April-2016, pp. 165-168 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Efficient Multi Server Authentication and Hybrid Authentication Method

Priya S. Birhade, Chaitanya V. Bhirud, Sangam D. Walke, Jyoti S. Borse

Abstract: - Password is used for authentication on many major client-server system, websites etc. Client and a server share a password using Password-authenticated key exchange to authenticate each other and establish a cryptographic key by exchanging generated exchanges. In this scenario, all the passwords are stored in a single server which will authenticate the client. If the server stopped working or compromised, for example, hacking or even insider attack, passwords stored in database will become publicly known. This system proposes that setting where multiple servers which are used to, so that the password can be split in these servers authenticate client and if one server is compromised, the attacker still cannot be able to view the client's information from the compromised server. This system uses the Advance encryption standard algorithm encryption and for key exchange and some formulae to store the password in multiple server. This system also has the hybrid authentication as another phase to make it more secure and efficient. In the given authentication schema we also use SMS integration API for two step verification.

1. INTRODUCTION

Password based user authentication systems are popular and low cost to apply and easy to implement . A user only needs remember a short password and can be authenticated easily anytime, regardless of the types of access devices users employs. Password based authentication system is still gaining popularity even in the presence of several alternative strong authentication approaches like biometrics authentication as they requires additional devices. The use of strong passwords is essential in order to protect your identity from attackers as there may be a chance of thefts. Unfortunately, many systems are designed that entirely relies on a password for security. Many researchers has found that 85percent of all passwords could be ordinarily broken through a simple thorough search to find short passwords and by using a dictionary. So, keeping passwords secured is important aspect. Most of the password authentication schemes assume the single-server to save passwords, hence as this server gets compromised all the passwords are revealed. The server is compromised by dictionary attack or SQL injection attacks. So to avoid such a problem we are giving solution of efficient multiple server password authentication system with hybrid authentication scheme mobile verification. In this system, user is secured by using multiple server password authentication process. When user enters the password, it will get spitted and stored in server using SOAP (Simple Object Access Protocol). At web Server the password is encrypted using AES KEY exchange protocol. Password split and distributes that password among multiple servers. So that, when attacker attacks the server, he able to get insufficient encrypted information. In previous system, there was single server system where all the passwords were stored which was a vulnerable system .If that server gets compromised then all passwords were disclosed. Passwords can be easily cracked because of single point failure. In this system the password gets encrypted first then gets store in multiple server instead of single server to remove disadvantage of single server system. All these server communicate through messages to authenticate client. But there was some kind of risk to store password with sequence only on two servers. We are extending this work by introducing multiple servers with better

security by splitting password as per servers then distribute that password randomly on them. And also by introducing the concept of two step verification.

2. RELATED WORK

In 2005, Katz proposed the first two-server password-only authenticated key exchange protocol with a proof of security in the standard model. Their protocol extended and built upon the Katz-Ostrovsky-Yung PAKE protocol called KOY protocol for brevity. In their protocol, a client C randomly chooses a password pw, and two servers A and B are provided random password shares pw1 and pw2 subject to pw=pwd1+pwd2. At high level, their protocol can be viewed as two executions of the KOY protocol, one between the client C and the server A, using the server B to assist with the authentication, and one between the client C and the server B, using the server A to assist with the authentication. The assistance of the other server is necessary since the password is split between two servers. In the end of their protocol, each server and the client agree on a secret session key. Katz protocol is symmetric where two servers equally contribute to the client authentication and key exchange.

Built on Brainerd in 2005, Yang suggested an asymmetric setting, where a frontend server, called service server(SS), interacts with the client, while a Back-end server, called control server (CS), helps SS with the authentication, and only SS and the client agree on a secret session key in the end. They proposed a PKI-based asymmetric two server PAKE protocol in 2005 and several asymmetric password-only two-server PAKE protocols in 2006. In their password-only protocol the client initiates a request, and SS responds with B =B1B2; where B1 = g1(b1)g2(1) and B2=1(b2)g2(2) are generated by SS and CS on the basis of their random password shares 1 and 2, respectively and then the client can obtain g1(b1+b2) by eliminating the password(=1+2) from B, i.e. computing B=g2. Next, SS and the client authenticate each other by checking if they can agree on the same secret session key, either g(1ab1+b2) or g1(aa1(b1+b2)); with the help of CS, where a, (a1; b1) and b2 are randomly chosen by the client, SS and CS, respectively. The security of Yang protocol is based on an assumption that the back-end server cannot be compromised by an active adversary. This assumption was later removed at the cost of more computation and communication rounds. Efficiency for practical use. Yang protocols are more efficient than Katz protocols in terms of communication and computation complexities, Its protocol structure which requires two servers to compute in series and needs more communication rounds.

In 2007,Jin further improved Yang protocol and proposed a two-server PAKE protocol with less communication rounds. In their protocol, the client sends the client, where H is a hash function. Next, SS and the client authenticate each other by checking if they can agree on the same secret session key g1(ab2b3); where a; (b1; b3); b2 are randomly chosen by the client, SS and CS, respectively. It needs less communication rounds than Yang protocol without introducing additional computation complexity. Its protocol structure which requires two servers to compute in series.

3. PROPOSED WORK

To overcome the drawback of existing system, we are developing an authentication system which is far secured than system which uses single server as an database for storing password and also than the system which have only password based authentication methods. We are proposing a new symmetric solution for multi-servers. To authenticate user on a network, the user usually need to provide his or her user id and password. Based on our multi-server PAKE protocol, we can split the user password into numbers of parts. This password will get split randomly according to the number of servers and get stored. So, In this system the attacker has an additional burden for compromising the servers in order to hack the system. System also detects the attackers when the attacker is trying to authenticate in system by inserting random characters as an password. As mentioned earlier this system will also contain the hybrid authentication method to make it more reliable and secured. The main reason to use of hybrid authentication is that proposed system will give authentication though the seventy percent or more than that of the password entered while login gets matched. Another reason of using the hybrid authentication is that there will be no chance of attacks like shoulder surfing or password guessing as the elements in matrix will get shuffle every time. For this some for the formulae are defined below for splitting the password randomly. Detailed implementation of modules is explained below:

3.1. Registration Phase:

For authentication, each client is need to register first. The user will enter his password which will be minimum of 8 character and also his phone number for mobile verification also with these details he will enter secret password for hybrid authentication steps. The password will get split in following way in number of servers:

Consider,

Val = number of characters in server 1,2,3,4 respectively,

Password= P

Step1:- Val1 = P length/2

Where, If val1 < 2

then val1 = 2.

Step2:- Val2 = P length - Val1 - 4

Where, If Val2 < 4

then Val2 = 2

Step3:- Val3 = P length - Val2 - Val1 - 2

Step4:- Val4 = P length - Val3 - Val2 - Val1

This above equation will split the password into random number. After splitting the password this split will get encrypted with same key for each server and stored in those servers.

3.2. Login Phase

While login user will enter his username and password. For this sytem need to retrieve that password from number of server to forms combination for checking matching character. In this phase the entered password is divided into numbers of shares according to the random number and various combination will be formed as follows:

Consider,

n = number of password character

s = number of servers

now,

Step1: Combination Ci= 2s -1

As our system is proposing that authentication will be given though the 70 percent or above of the entered password gets matched. So for this it is needed to check whether the password entered by user while authentication matches 70 percent criteria. Following equations will help to find percentage match for each combination and will check the maximum matching percentage as If password is matched at least 70 percent or more it would be considered as valid and authentication is permitted.

Step2: Pi = Ci / n

Where, Pi= Percentage of character match in combination.

MAXi = Maximum Value match in Combination

Now,

Step3: MAXi = MAX Pi

If, MAXi >= 70per

If MAXi is greater than or equal to seventy percent authentication will be given. After this user will go for hybrid authentication which is explained in next phase.

3.3. Hybrid Authentication Phase

While registering the user also have to enter his secret password which will be of even numbers of characters in length. During authentication user, when he or she will come to this step there will be matrix of 6X6. In this matrix there will be 36 elements which will be the combinations of 26 alphabets and numbers from 0-9. Every time these elements will randomly get shuffled in matrix. Now the actual working is as follows-.As the secret password is of even numbers in character, user has to consider in terms of pairs. The first letter in the pairs is used to select the row element and the second letter is used to select the column element in the 6X6 matrix to find intersection. The intersection element which is selected generated session key. This logic is used for every pair of secret password. Thereafter, the password inputted by the user is now verified by the server to authenticate the user.

3.4. One Time Password

After both of the above steps user will receive one time password on his registered mobile number. User will have to verify this password so as get authentication. For this we are using msg.message.net API of Java.

5. CONCLUSION

As, there are many drawbacks with the passwords such as brute force and dictionary attacks. Same is the case with the graphical passwords which are guessed by shoulder surfing and are not cost effective to implement. It is Efficient for practical use. The project will provide an efficient and secure Multi-server password authentication system along with mobile based validation system. By employing multiple servers, the system is able to offer more safeguard to sensitive user data than any single database server approach could permit. For making it more secure we had used two techniques such as textual and graphical password techniques. For future work, as hybrid authentication technique is new to the user can also be developed as windows application such as a folder locker or an external gateway authentication to connect the application to a database or an external embedded device.

5. FUTURE SCOPE

This Paper has two methods of authentication based on matrix as well as password is mentioned which we have implemented for web applications or for databases. These techniques can be further used for PDA's. One of these techniques are resistant to shoulder surfing, brute force attacks, dictionary attacks etc. Hybrid authentication schemes is completely new to the users this techniques should be verified extended for usability and effectiveness. These techniques can also be developed a folder locker or for an external embedded device.

REFERENCES

[1] S.A.Deshpande, Pawar Vishal, Rane Ashwini, Gite Supriya "Multi Server Password Authentication by Key Exchange Protocol in Secure Manner", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 4, April 2015.

[2] VIGNESH KUMAR K, ANGULAKSHMI T, MANIVANNAN D, SEETHALAKSHMI R, WAMINATHAN P, "PASSWORD BASED TWO SERVER AUTHENTICATION SYSTEM", Journal of Theoretical and Applied Information Technology, vol-39, May 2012.

[3] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini,V.Venkateswara Reddy, " UTHENTICATION TECHNIQUES FOR ENGENDERING SESSION PASSWORDS WITH COLORS AND TEXT".

[4] Lekha Deshmukh, Ankita Kathale, Sayali Kulkarni,Prof. Smita Chaudhari,"Password Authentication Using Two Server Key Exchange", International Journal of Engineering and Technical Research (IJETR),Volume-3, March 2015.

[5] M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols", Proc. Intl Conf. Topics in Cryptology (CT-RSA),2005.

[6] J. Katz, P. MacKenzie, G. Taban, and V. Gligor, "Two Server Password-Only Authenticated Key Exchange,' Proc. Applied Cryptography and Network Security(ACNS)",2005.

[7] Y. Yang, F. Bao, and R.H. Deng, A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprise.

[8] Brainard,A. Jueles, B.S.Kaliski,and M.Szydlo, "A New Two Server Approach for Authentication with Short Secret".

