International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 2, Issue 6, June 2014)

# Password Authentication Key Exchange By Two Server Password Only in Web Applications.

Rupali Zamare[1], Prof Rajesh Phursule[2]
[1]ME Comp, [2]Asso. Professor, Department of Computer Engg, ICOER, University of Pune

*Abstract*--**In the world of communication there is need of secure transmission of message so password based authentication make a client and a server to authenticate and established a session key through Deffie Hellman and ElGamal protocol. In single server architecture, passwords are stored in single server only, if it got hacked through attack, the password will get easily accessed by the intruder .To solve this problem two server with password authenticated key exchange is used where symmetric or asymmetric way is applied .So in the symmetric protocol which is used to initialized our secure transmission ,client can form cryptographic keys in two servers. The efficiency of protocol is better ,It is cost effective and lead to parallel execution of servers which are included for registration and authentication.**

***Index Terms*—Deffie Hellman protocol, ElGamal encryption, two passwords only**

## I. INTRODUCTION

Hacking and intrusion are the major problems in secure transmission of messages between server and client, which can be easily done through comprimisation of server. One other way to break the security is by guessing the passwords also the hash values can be guessed which the easiest way is for attacker which is commonly used or followed by most. Preliminary studies cover the concept of online and offline attacks ,majorly they are grouped under dictionary attacks. Here offline attacks are faster in speed of guessing the password. Offline attacks are the passive attacks in which attacker try to guess the password from the conversation or communication made between two parties and guess the attacks from the dictionary. Online attacks the attacker guess the password through dictionary and tries to login. Online attempts made to guess the password is also called as active attacks .These both types of attack should be avoided in client server communication. The main aim in server and client architecture is that client's passwords are maintained to server only. When that server gets hacked then security in the transmission of message will be reduced.. The architecture which is best suited is the public key Infrastructure and the model used is PKI model.

PKI model is used for password protection. It enables users to securely and privately exchange data with the use of public and private key pair. The digital certificate .It uses the public key cryptography. The password only authenticated key exchange uses short password of user.

The second model which is password only model, where password is the secret key for encryption of random selected numbers which is considered as a benchmark for the cryptographic assumption. Here the main concept is the user has to remember the password every communication done is based on important factor that is password as it doesn't require any external storage.

## II. LITERATURE REVIEW

The base paper [1] has proposed the protocol which is based on deffie hellman and the ELGamal protocol thus increasing the complexity and making the protection of client and server stronger.In paper [3] author introduced password based authentication protocol with the help of two protocols out of which one is concentrating on where password is shared among several servers and second protocol is security efficient . Random oracle use is avoided. SPAKE 1and SPAKE 2 protocol is used for security and to solve the problem of computational Diffie Hellman which is called as chosen basis Computational Diffie Hellman assumption.

In paper [7] author introduced the two servers are used with the protocol like EKE and SPAKE.SPAKA helps to avoid the leakage in password. Password can get recovered due to the proposed protocol. The replay and testing of communication through the protocols is making the implementation stronger which consists of red and blue server where blue work as control and red as service server. Here as compared to one server working the two servers can handle the cryptographic protocols.

In paper [6] the client server with the password sharing among multiple servers can be done hence it is efficient and implementable protocol. The KOY protocol assigns the security for the threshold in the security and the transparent protocol adds the transparency in the protocol. Here the passwords can be protected against the hacker's attacks.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 2, Issue 6, June 2014)

In paper [8] password authentication protocol based on RSA, where verification information is used along with the password so the strong shared session key is generated with the SNAPI and SNAPI-X protocol.If server get compromise due to attacker he may try to get the password along the identification of information but won't be able to impersonate as a user. Thus through RSA and the use of extended protocol security of password get maintained.

In paper [4] the author has initiated the use of short passwords for authentication and key exchange. In federated organizations one external server is assigned which is managed by the individual enterprises and the main central server which is controlled by headquarters of enterprise. The federated enterprises are in picture due to expansion in the market. The offline attacks are eliminated by the special architecture where password is transformed into two long secrets. In paper [5] author has given the idea of identity based encryption which consist of setup,extract,encrypt and decrypt phases.The system consist of bilinear maps between the groups. The weil pairing is an example of maps.

The chosen identity based computation makes cipher text secure with the ELGamal encryption scheme.

In the paper [9] author has introduced protocols which secure the password and also avoid the offline dictionary attacks due to which intruder or hacker find it difficult to guess .Author have used direct authentication protocol, secret public key protocol, nonce protocol, identification protocol, enhanced Kerberos protocol, compact protocol, demonstration protocol, mutual authentication protocol are used in password protection technique. Protecting poorly chosen passwords from guessing attacks.

In paper [2] author mentioned the need for multiserver Medicare systems is initiated because one server or two servers becomes inefficient to handle the situation where no of services are required to pass on to the customers and need to get equally maintained and updated. Where one password can get shared in multiple servers where user can login to different servers for services requests. Thus the organizational structure will get maintained in the health care system.

## III. EXISTING SYSTEM

The existing protocols are symmetric one is koy protocol with the proof of security and it increases the efficiency of original koy protocol.

But the major disadvantage is it is not taking into account the offline computation or pre computation while the yangs protocol use the asymmetric two server password only protocol where one of the server authenticates the client with the help of other, also in the Jin's protocol structure requires two servers to compute in series.

*Deffie Hellman Protocol*

This is the basic protocol used in cryptography where the two users. It is secure because is complexity is in the form of discrete logarithms in a finite field in comparison with the exponentiation in the same one. The two users like to have secure communication between them so Deffie Hellman key exchange protocol is used as follows:-

1. Alice and bob as the two users agree on the cyclic group G having large prime order q with a generator g.

2. Alice randomly chooses an integer a from $Z_q^*$and X $= g^{ab}$ and meanwhile bob chooses a integer b from $Z_q^*$ calculates $Y = g^b$ .After this the two users exchange X and Y.3.Alice will do the calculations for the secret key $k_1 = Y^a = g^{ab}$.Bob calculates his secret key as $k_2 = X^b = g^{ab}$ It is clear that both secret keys i.e.

Bob side and Alice side key is same through which secure communication can be done .Diffie Hellman is most secure against passive adversary. The Computational Deffie Hellman(CDH) and Decisional Deffie Hellman assumptions are required to built the security are as follows:-Consider the cyclic grouping G of large prime number order q with

a generator g.CDH states that a given $(G,g,g^a,g^b)$

for randomly chosen a,b from $Z_q^*$ it is computational yz intractable to compute the value $g^{ab}$.

For Decisional Deffie Hellman consider the cyclic grouping G of large prime order q with a generator g.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 2, Issue 6, June 2014)

It state that given (G, g,$g^a$ ,$g^b$ )for randomly chosen a,b from $Z_q^*$ no Probabilistic polynomial time algorithm can distinguish the following two probability distributions with probability more than ½ plus a negligible value :- ($g^a$,$g^b$,$g^{ab}$) where a and b are taken randomly independent from $Z_q^*$($g^a$,$g^b$,$g^c$ )where a,b,c are taken randomly and independently chosen from $Z_q^*$

*ELGamal Encryption Protocol*

It is based on Diffie Hellman Protocol, where the main function of ELGamal is to keep the secure password from each other. The encryption process is used to make the security even stronger with the help of Deffie Hellman. There are three main components in Elgamal encryption protocol. First Key generation:-k is used as an input and it establish a cyclic group G where it consists of prime. Order q with generator g, where x is the key for decryption from $Z_q^*$ also encryption key generated is

$$y=g^x$$

*Second Phase Encryption:*-As it is getting message is input also it one more input is from the key generation phase for which the cipher text generated as C=epsilon (m, y) = (A, B) = ($g^r$, m.yr)

*Third Phase Decryption:*-As we are getting cipher text (A, B) and the key of decryption which is giving the output as m=D(C, x) =B/$A^x$.

The main property of ELGamal is concentrating around the probability function which is secure and follows the DDH assumption and has some properties which are as homographic.

## IV. PROPOSED SYSTEM

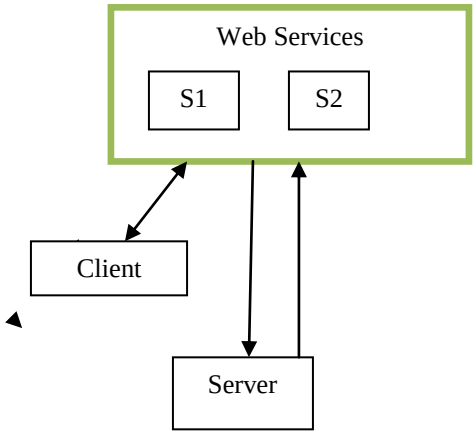


FIG 1 SYSTEM ARCHITECTURE

The proposed system consists of client server architecture where the two servers used as web services where server $S_1$ and server Server $S_2$ and the third web server will do the communication with the client. If one of server in the web services is compromised then the second server will block the attack which may be active attack or passive attack and will do the transmission securely of message. Thus the second server will maintain the continuous communication between the server and client. This system is helpful in fields like federated organizations, medical care institutes and different web servers. The proposed system work on three main phases listed as follows:-

*Phase I Initialization*

In this phase the two servers $S_1$ and $S_2$ select the cyclic group G with generator $g_1$ with the hash function H:{0,1}*→ $Z_q$(Message of length l=$\log_2$q).The $S_1$ an integer $s_1$ from $Zq^*$

And $S_2$ selects $s_2$ from $Zq^*$ and the two servers exchange the generated values.Thus the both the servers publish the public parameters.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 2, Issue 6, June 2014)

*Phase II Registration*

After initialization the protocol follows the registration phase which is followed by the authentication. Both the servers $S_1$ and server $S_2$ adopt the channels which are secure. Our client C forms the keys for encryption and decryption with the pairs $(x_{i,}\ y_i)$ for server. Then the client C chooses a password $P_{WC}$ and encrypts the password using the encryption key which will be done through ELGamal encryption.

At the end client C generate the password authentication for the respective servers and client C only keeps the information about the $P_{WC}$

Phase III Authentication After receiving the information about authentication by the client in registration phase. The authentication diagram of containing five steps show that both servers work simultaneously in every step thus maintain the parallel execution of the whole process of authentication. Hence the required computation period is also less.

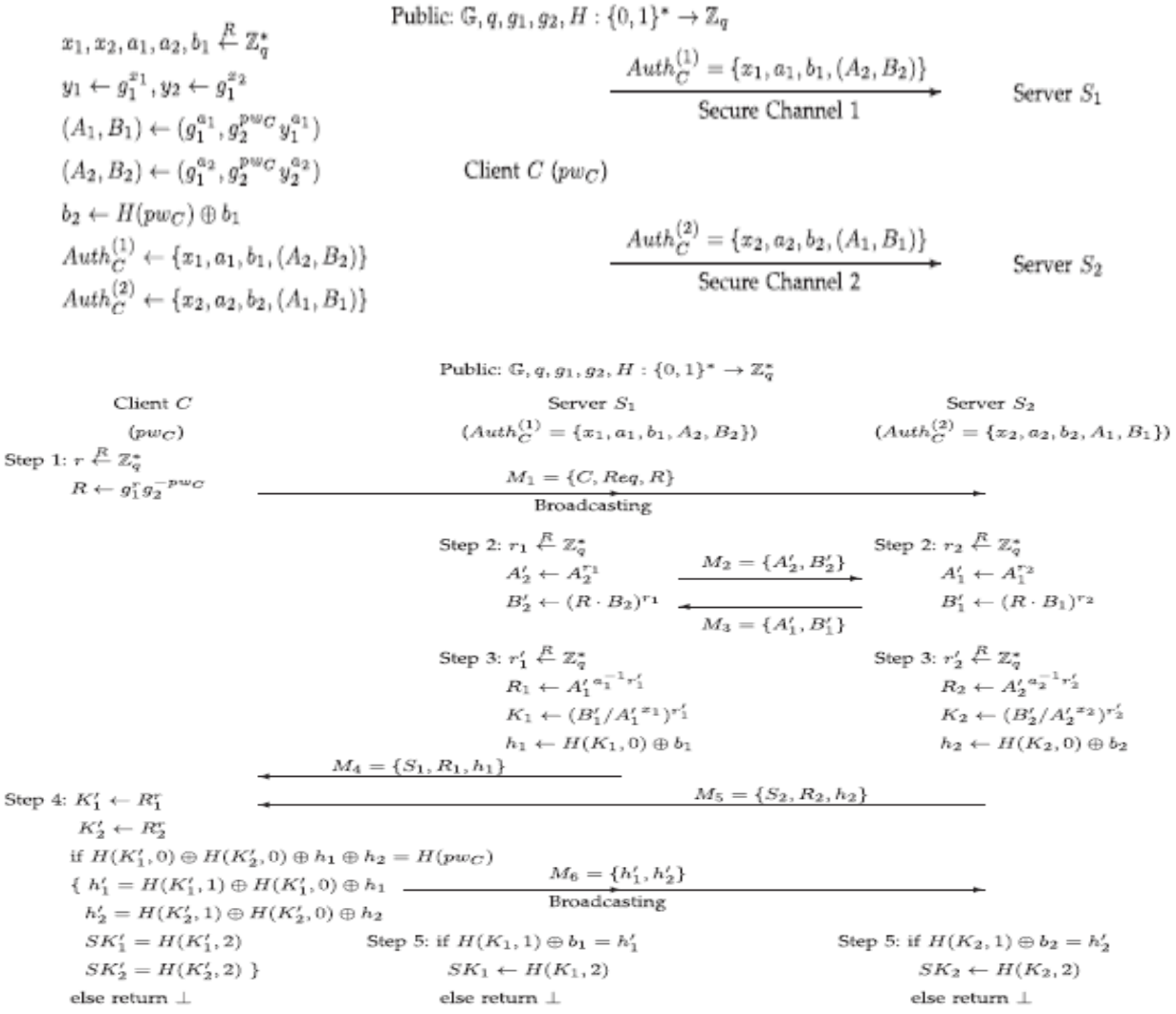


**Fig. 2 Registration and Authentication of Protocol**

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 2, Issue 6, June 2014)

## V. Results Of Implementation

The proposed system is implemented successfully by having the first page as the login page where the authenticated client get registered and the client password get divided among two servers $S_1$ and $S_2$.

*Phase Registration and Authentication:-*

If the entered username and email id are from the authenticated user which is checked with the local database then registration is done for example if rupali username and email id as rupalizamare@yahoo.com with the password to register. Then authentication information can be divided as

Authentication (1) = {61,271,521(30, 25191)}
Authentication (2) = {163, 499, 2136, (269,250)}

The result of registration is that Server $S_1$ and $S_2$ are authenticated.

Where the values of encryption and decryption key at server1 along with the random value, key value and hash value are:-

$A_2$' = 163
$B_{2'}$ =163
$R_1$ = 0
$K_1$ = 0
$H_1$ = 0

Where the values of encryption and decryption key at server 2 along with the random value, key value and hash value are:-

$A_1$' = 239
$B_{1'}$ =239
$R_2$ = 0
$K_2$ = 0
$H_2$ = 0

Then the authentication of the client is done at both the server side where if the client put his or her the username and password correctly with the help of segregate session key. If the client is not providing the correct password then authentication is not done. This is the best policy for protecting the transaction on client and server side.

*Result Table:-*

| **Server 1** | **Server 2** |
|---|---|
| $A_2$' = 163 | $A_1$' = 239 |
| $B_{2'}$ =163 | $B_{1'}$ =239 |
| $R_1$ = 0 | $R_2$ = 0 |
| $K_1$ = 0 | $K_2$ = 0 |
| $H_1$ = 0 | $H_2$ = 0 |

The authenticated client is able to carry out the further transaction of passing message through server 1 successfully by using the upload a file option. Like this implementation is proved to be successful through initialization, registration and authentication phase.

Now if we again put the same password and username for registration phase then at every entry we will get different set of encryption and decryption keys,which is tough to get break by the intruder.

## VI. Conclusion

The protocol which will be used in proposed system gives the password authentication .Key exchange in a secure way. The communication of two servers is symmetric and computation rounds are less due to parallel working of two servers whose comprimization is avoided on the basis of the assumption in DDH and CDH.Thus the system is secure against the active and passive attack thus increasing its efficiency.

## REFERENCES

[1] Xun Yi, San Ling, and Huaxiong Wang ,"Efficient Two-Server Password-Only Authenticated Key Exchange",IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 9, September 2013

[2] Y. Yang, R.H. Deng, and F. Bao, "Fortifying Password Authentication in Integrated Healthcare Delivery Systems," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), pp. 255- 265, 2006.

[3] M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.

[4] Y. Yang, F. Bao, and R.H. Deng, "A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprise," Proc. 20th IFIP Int'l Information Security Conf. (SEC '05), pp. 95-111, 2005.

[5] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586-615, 2003.

[6] M. Di Raimondo and R. Gennaro, "Provably Secure Threshold Password Authenticated Key Exchange," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt '03), pp. 507-523, 2003.

[7] J. Brainard, A. Jueles, B.S. Kaliski, and M. Szydlo, "A New Two-Server Approach forAuthentication with Short Secret," Proc. 12th Conf. USENIX Security Symp., pp. 201-214, 2003.

[8] P. MacKenzie, S. Patel, and R. Swaminathan, "Password-Authenticated Key Exchange Based on RSA," Proc. Sixth Int'l Conf. Theory and Application of Cryptology and Information Security: Advances inCryptology (Asiacrypt '00), pp. 599-613, 2000.

[9] L. Gong, T.M.A. Lomas, R.M. Needham, and J.H. Saltzer, "Protecting Poorly-Chosen Secret from Guessing Attacks," IEEE J. Selected Areas in Comm., vol. 11, no. 5, pp. 648-656, June 1993.