International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-3 Issue-4, September 2014

An Efficient Key Exchange Authentication Using Browser Based Security

U. Siva Kumari, M. S. S. Sai

Abstract: ***Password-authenticated key exchange (PAKE) is where a client and a server, who share a password, authenticate each other and meanwhile establish a cryptographic key by exchange of messages. In this setting, all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised, due to, for example, hacking or even insider attacks, passwords stored in the server are all disclosed. In this paper, we propose a browser based security and usage of two servers which cooperate to authenticate a client. Even if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server.***

Index Terms: ***Password, (PAKE), Messages, security,***

I. INTRODUCTION

Password Authentication is the most widely used method. Password based encrypted key exchange protocols are designed to provide users to communicate over an unreliable channel with a secure session key. These systems are easy to use and are low cost. Password authentication requires no dedicated devices like smart cards. Password based user authentication systems total trust is based on the authentication server, which performs password verification data (PVD) derived from central database. With the password the client authenticates himself to the server. The user can simply send the password to the server, which validates the received password [5], [6]. For security reasons, the password should be encrypted before it is transferred. Passwords are easy to remember but inherently weak because most passwords are selected from dictionary, so it allows for brute-force attacks called dictionary attacks [13]. The attackers try from different browsers and different IP with possible password from dictionary. Dictionary attacks are classified as offline and online attacks. In case of online attack, attackers attempt to log in to the server by trying all passwords from dictionary, but in case of offline attack; attackers store all past successful login session between a user and a server and then check the passwords in the dictionary against the login transcript [3], [8]. In the most rigorous password-only security models, there is no requirement for the user of the method to remember any secret or public data other than the password [19]. Most password-based authentication systems employ a Secure Socket Layer (SSL) connection is established first between the client and the server and then a password is sent to the server via SSL connection for client-side authentication. Since each SSL session establishes a random session key by which the password is encrypted, if an attacker eavesdrops the encrypted password, attacker will not be able to replay it. The two server systems that are available for password authentication exposes one server to users and the other is hidden from public. In the proposed system the hidden server is made public there by the number of users are increased by two way authentication and also by efficiently using the control server.

Password-authenticated key exchange (PAKE) is where a client and a server, who share a password, authenticate each other and meanwhile establish a cryptographic key by exchange of messages [13]. In this setting, all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised, due to, for example, hacking or even insider attacks, passwords stored in the server are all disclosed. In this paper, we propose a browser based security and usage of two servers which cooperate to authenticate a client. Even if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server [17].

Revised Manuscript Received on 30 September 2014.
* Correspondence Author
U. Siva Kumari*, M.Tech. Student, Department of CSE, KKR & KSR Institute of Technology & Sciences, India
Dr. M.S.S. Sai, Professor, Department of CSE, KKR & KSR Institute of Technology & Sciences, India

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

II. AUTHENTICATION MECHANISM

In Two server systems, the user is allowed to communicate with single system, public server where as the other system is the back-end server or the control server used for authentication only. The important difference between the two server and the multi server models: A user ends up establishing a session key only with the public server where in multi server model a user establishes a session key with each of the servers [9]. In addition, the server keeps track of the browser being used by the user and also the system related information. Next time when the user try to login, it verifies with the information stored with the earlier successful login attempt. It the information does not match, and then the server ask the user for some security questions at random. If the answer is correct then the login will be successful and the current information will be updated in the server.

III. BASIC PASSWORD AUTHENTICATION AND KEY EXCHANGE PROTOCOL

System Model

The three entities that are involved in the system are the users U , Service server SS , and the control server CS . The service server is the public server and the control server is the hidden back end server in the two server model [7].

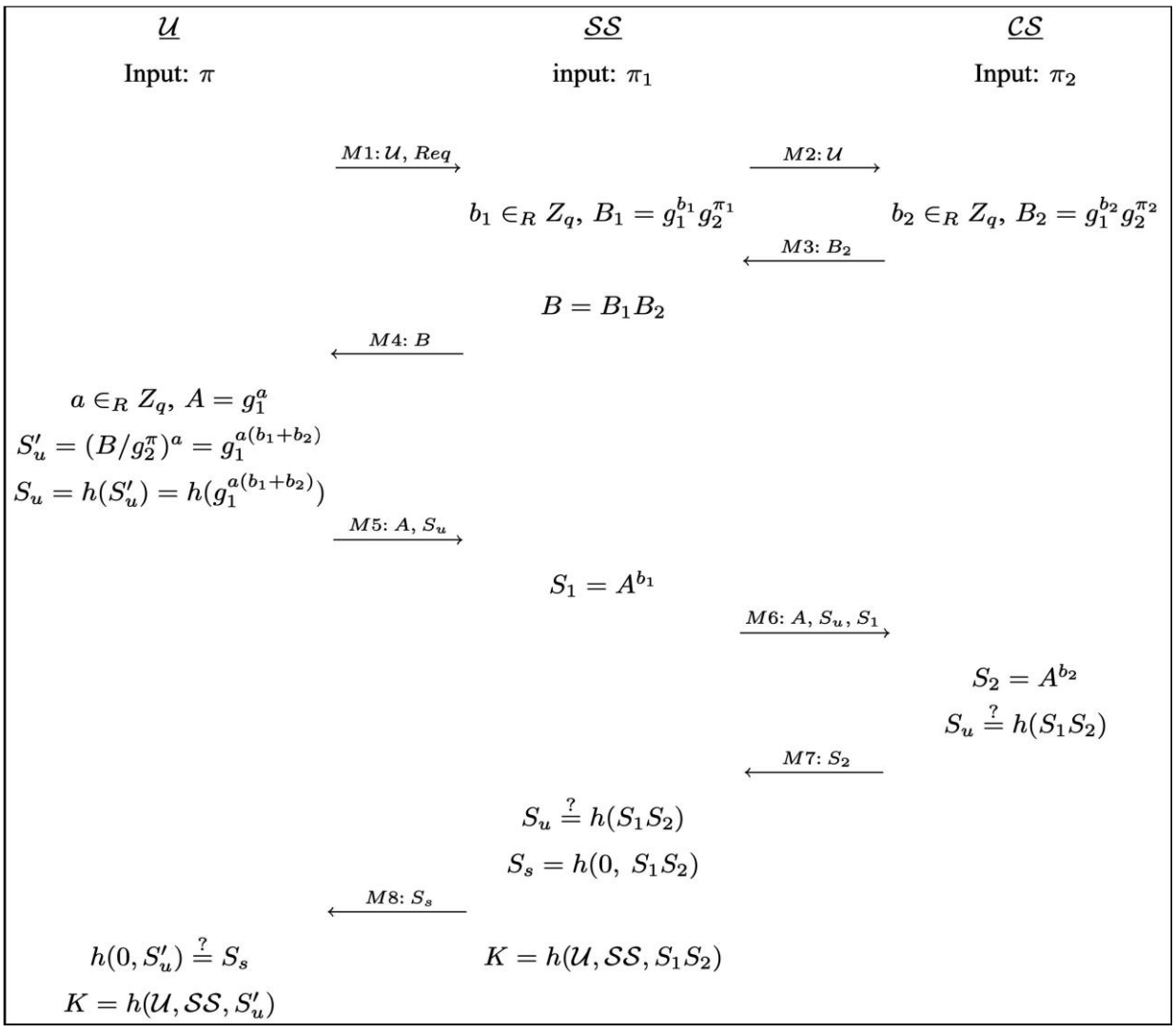
Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved

In this protocol the users can only communicate with the public server and the control server is away from the users [9], [13]. Users are not aware about the control server and it is especially used for user authentication. The user's long secrets passwords are transformed into two secret passwords which are held by public server and the control server. The two server based on the secret passwords validate the user while login [18].

The user must beforehand register with the servers by establishing a shared password. The password π is divided as π_1 and π_2 the long random numbers such that $\pi_1 + \pi_2 \bmod q$, where q is the prime numbers. The passwords are stored in the two servers with the user id and the password as (U, π_1) and (U, π_2) respectively. U registers π_2 to control server CS through postal mail. To initiate a request for the server, user U sends his identity together with a service request $\mathrm{Re}\, q$ to $Server1$ in $M1$ [5], [7], [13], [16].

User Registration

Basic Password Authentication Protocol The mutual authentication and key Exchange enables between user and public server SS. We outline the basic password authentication protocol here. The notations and symbols followed are tabulated in table below.



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved

The user initiates the request after completing the user registration phase with the SS in message $M1$.The SS sends the request to CS with the user id in $M2$ [3], [12]. Then SS computes the value of B_1 by selecting a random number b_1 from the set z_q .The CS selects the random number b_2 from the set z_q to compute the value of $B_2 = g_1^{b_2} g_2^{\prod_2}$ .We omitted the modulo p notation for arithmetic operation. The CS sends the value B_2 to SS in $M3$. SS now computes B and sends to user U in $M4$. The U selects the random number a from the set z_q and computes the following values $A = g_1^a$ $S_u^{'} = g_1^{a(b_1+b_2)}$ and $S_u = h(g_1^{a(b_1+b_2)})$ then sends A, S_u to SS in $M5$. The SS computes S_1 then passes A, S_u and S_1 to CS in $M6$. The CS computes S_2 and S_u checks the value of S_u to authenticate the user and then passes S_2 to SS in $M7$. The SS computes S_u and S_s, it checks the value of S_u and authenticates the user. The session key K is established between the SS and U . The SS sends the value of S_s to U in $M8$. The U also authenticates the SS by comparing the values of S_s . Thus, the basic protocol works where both the server and the user authenticate each other and establishes the connection [4], [10, [19].

IV. PROPOSED PASSWORD AUTHENTICATION AND KEY EXCHANGE PROTOCOL MODULE

The three entities that are involved in the system are the users U , Service server SS , and the control server CS . The service server is the public server and the control server is the hidden back end server in the two server model. In this protocol the users can only communicate with the public server and the control server is away from the users. Users are not aware about the control server and it is especially used for user authentication [3], [4], [16]. The user's long secrets passwords are transformed into two secret passwords which are held by public server and the control server. The two server based on the secret passwords validate the user while login.

User Registration

The user must beforehand register with the servers by establishing a shared password. The password π is divided as π_1 and π_2 the long random numbers such that $\pi_1 + \pi_2 \bmod q$, where q is the prime numbers. The passwords are stored in the two servers with the user id and the password as (U, π_1) and (U, π_2) respectively. U registers π_2 to control server CS through postal mail. To initiate a request for the server, user U sends his identity together with a service request $\mathrm{Re}\,q$ to $Server1$ in $M1$.

Proposed Password Authentication Protocol

We propose a mechanism in which we verify for the browser and the IP address of the client machine. After verification the mutual authentication and key Exchange enables between user and servers $Server1$ and $Server2$. We outline the proposed password authentication protocol here. The user initiates the request after completing the user registration phase with the servers $Server1$ or $Server2$ in message $M1$. If the user request $Server1$, then $Server1$ computes the value of $f(x) = x^a \bmod n$, $U^{'} = h(\prod_1)[f(x)]$ and $V^{'} = h(\prod_1)[x]$. $Server1$ sends $uid, U^{'}, V^{'}$ to $Server2$ in $M2$.

$Server2$ decrypts using the hash that is stored in the database to obtain f(x) and x. $Server2$ then computes $g(x) = x^b \bmod n$,, $g(y) = y^b \bmod n$, $g(x,y) = (xy)^b \bmod n$, $k = (f(x) * g(x)) \bmod n$ and $U^{''} = h(\prod_2)[g(x), g(y), g(x,y)]$. $Server2$ sends the $U^{''}, k[x,y]$ to $Server1$ in $M3$. $Server1$ computes $k = (f(x) * g(y)) \bmod n$, $f(y) = y^a \bmod n$, $f(x,y) = (xy)^a \bmod n$ and $f(g(x,y)) = (g(x,y))^a \bmod n$. $Server1$ sends $f(y), f(x,y), f(g(x,y)), k[y]$ to $Server2$ in $M4$. $Server2$ checks the values $g(f(x), f(y)) \stackrel{?}{=} f(g(x,y))$ to authenticate the $Server1$. $Server2$ computes $B_2 = g_1^{b_2} g_2^{\prod 2} \bmod p$ meanwhile $Server1$ computes $B_1 = g_1^{b_1} g_2^{\prod 1} \bmod p$. $Server2$ sends $g(f(x,y)), B_2$ to $Server1$ in $M5$. $Server1$ computes and validates to authenticate the $Server2$ $f(g(x), g(y)) \stackrel{?}{=} g(f(x,y))$ and $B = B_1 B_2 \bmod p$. $Server1$ sends the value B to user U in $M6$. The user U computes $A = g_1^{a_1} \bmod p$, $S_u^{'} = (B / g_2^{\prod})^{a_1} \bmod p$ and $S_u = h(S_u^{'})$. The user U sends A, S_u to $Server1$ in $M7$. $Server1$ computes $S_1 = A^{b_1} \bmod p$ and sends the value A, S_u and S_1 to $Server2$ in $M8$. $Server2$ computes $S_2 = A^{b_2} \bmod p$ and authenticates the $Server1$ by checking the values of $S_u \stackrel{?}{=} h(S_1 S_2 \bmod p)$. $Server2$ sends the value of S_2 to $Server1$ in M9. $Server1$ computes

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved

$S_u \stackrel{?}{=} h(S_2^{A^{b_1}} \bmod p)$,

$S_S = h(A^{b_1 S_2} \bmod p)$, and

$K = h(uid, ser1, A^{b_1 S_2} \bmod p)$

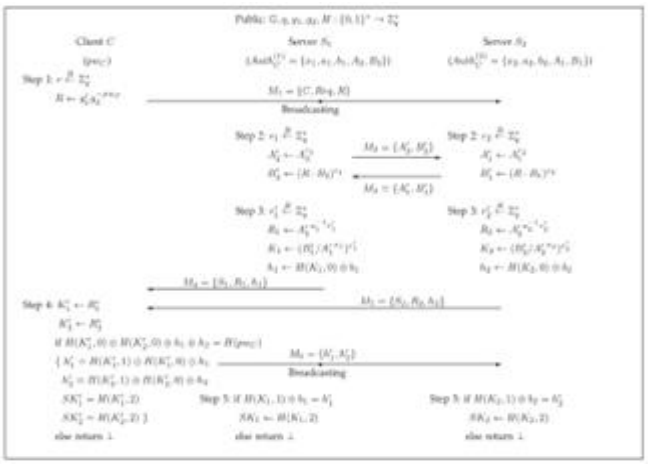
then passes the value S_s to user U in M10. The U also authenticates the *Server*1 by comparing the values of S_s. Thus, the basic protocol works where both the server and the user authenticate each other and establishes the connection.

Decisional Diffie-Hellman Assumption

Let p, q be the prime numbers and g, h $\in_R z_q$ of order q, for probabilistic polynomial time algorithm A, the following condition is satisfied:

$$Adv_G^{DDH}(A) = |\Pr[A(g,h,g^r,h^r)] - \Pr[A(g,h,g^r,z)]| < \in$$

Where $r \in_R z_q$, $\in_R QR_p$, and $\in$ is a negligible function. That is computationally intractable for A to distinguish between (g,h,g^r,h^r) and (g,h,g^r,z).



1. The protocol is robust against offline dictionary attacks by control server as a passive adversary.
2. When the control server is controlled by a passive adversary, the intruder may eavesdrop on the communication channels to collect protocol transcript and attacks against the password of the user. Control server can obtain B_1 from $M4$. The control server cannot know anything of π_1.
3. The protocol is robust against offline dictionary attacks by public server as an active adversary.
4. The public server is unable to learn on either π or π_2 from the two pairs. The values that are coming from user and control server are replaced and passed to other so it is secured from offline dictionary attacks.
5. The protocol is secure against an active outside adversary controlling no server.
6. From the user an adversary is no more effective than public server. In case for the public server it is impossible to compute the values from the secured hash function.

V. CONCLUSION

The proposed authentication system can be used instead of existing single server system such as FTP and email servers where the number of users can be increased by providing two way user authentication using two servers. The future work to be carried is designing the protocol in the wireless environment between users and servers and placing a back up third server when any one of the server fails. In this paper, we have presented a symmetric protocol for two-server password-only authentication and key exchange. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised.

REFERENCES

1. M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypte Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.
2. M. Abdalla, O. Chevassut, and D. Pointcheval, "One-TimeVerifier-Based Encrypted Key Exchange," Proc. Eighth Int'l Conf.Theory and Practice in Public Key Cryptography (PKC '05), pp. 47-64,2005.
3. M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated KeyExchange Secure against Dictionary Attacks," Proc. 19th Int'l Conf.Theory and Application of Cryptographic Techniques (Eurocrypt '00),pp. 139-155, 2000.
4. S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocol Secure against Dictionary Attack," Proc. IEEESymp. Research in Security and Privacy, pp. 72-84, 1992.
5. D. Boneh and M. Franklin, "Identity Based Encryption from theWeil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. (Crypto '01),pp. 213-229, 2001.
6. D. Boneh and M. Franklin, "Identity Based Encryption from theWeil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586-615, 2003.
7. D. Boneh, "The Decisional Diffie-Hellman Problem," Proc. ThirdInt'l Algorithmic Number Theory Symp., pp. 241-250, 1998.
8. V. Boyko, P. Mackenzie, and S. Patel, "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 156-171, 2000.
9. J. Brainard, A. Jueles, B.S. Kaliski, and M. Szydlo, "A New Two-Server Approach for Authentication with Short Secret," Proc. 12th Conf. USENIX Security Symp., pp. 201-214, 2003.
10. W. Diffie and M.E. Hellman, "New Directions in Cryptogra- phy," IEEE Trans. Information Theory, IT-22, no. 6, pp. 644-654, Nov. 1976.
11. 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.
12. T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.
13. W. Ford and B.S. Kaliski Jr., "Server-Assisted Generation of a Strong Secret from a Password," Proc. IEEE Ninth Int'l Workshop Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 176-180, 2000.
14. O. Goldreich and Y. Lindell, "Session-Key Generation using Human Passwords Only," Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (Crypto '01), pp. 408-432, 2001.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved

15. L. Gong, T.M.A. Lomas, R.M. N eedham, and J .H. S altzer, "Protecting Poorly-Chosen Secret from Guessing Attacks," IEEE J. Selected Areas in Comm., vol. 11, no. 5, pp. 648-656, June 1993.
16. S. Halevi and H. Krawczyk, "Public-Key Cryptography and Password Protocols," ACM Trans. Information and System Security,vol. 2, no. 3, pp. 230-268, 1999.
17. D. Jablon, "Password Authentication Using Multiple Servers," Proc. Conf. Topics in Cryptology: The Cryptographer's Track at RSA (RSA-CT '01), pp. 344-360, 2001.
18. H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password-Only Two-Server Authenticated Key Exchange System," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.
19. J. Ka tz , R . O st rovs ky, and M. Yung, " Ef ficient P a sswo r d-Authenticated Key Exchange Using Human-Memorable Pass- words," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (Eurocrypt '01), pp. 457-494, 2001

© Copyright: All rights reserved