ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 310 - 315 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

AN EFFICIENT KEY EXCHANGE AUTHENTICATION USING BROWSER BASED SECURITY

T.ANUSHA[1], S.AMARNATH BABU [2]

[1]II year M.Tech, St. Ann's College of Engineering & Technology, Chirala India,anusha.thota51@gmail.com
[2]Associate professor, St. Ann's College of Engineering & Technology, Chirala, India, amardots@gmail.com

Abstract: Password key exchange is a client and a server, who share a password, authenticate each and every one that is client and server determining a cryptographic key by change of text message. the passwords necessary for authenticate clients are stored in a single server. If the server is compromised, 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. if one server is compromised, the attacker still cannot pretend to be client with the information from the compromised server.

INTRODUCTION

Authentication is the most used method. Password based encrypted key exchange protocols are designed to provide clients to communicate over an unreliable channel with a secure session key. The Password authentication required no dedicated to the devic 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. 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.

The attackers try different brows and different IP adderess with possible password from dictionary. Dictionary attacks are classified to offline and online attackers. In the case of online attack, attackers attempt to log in to the server by trying all passwords from dictionary, but in the case of offline attacks; attackers store all past successful login session between a user and a server and then check the passwords in the dictionary against the login transcripts. In the most rigorous passwords security models, there is no requirement for the user of the method to remember any secret or public data other than the password.

Most password based on the authentication systems employ a Secure Socket Layer connection is established first between the client and server then a pass is sent to the server via Secure Socket Layer connection for client-side authentication. Since each Secure Socket Layer session establishes a random session key which the password is encrypted, if an attacker eavesdrops the encrypted password, attacker not be able to replay it. The two server systems that are available for pass authentication exposes one server to users and the other is hidden from public. In the proposed system the hidden server is made by the number of users are increased by two authentication by efficiently using the server.

Current solutions for password based authentication follow 2 models. The first model called as one is PKI-based model, assumes that the client keeps the server's public key in addition to share a password with the server. The second model is called password-only model. The first consider authentication based on password only introducing a key of so called"encrypted key exchange"protocols,where the password is used as a secret key to encrypt random number for key exchange purpose.

Problem Statement :

One of the Most password-based client authentication systems place total trust on the authentication server where clear text passwords or easily derived password verification data stored in a central database. Such systems are, thus, by no means resilient against offline dictionary attacks initiated at the server side..

Description of Organization:

The Passwords are the most common method for authentication used to the control access to digital resources. They are also the easiest way to gain unauthorized access to these resources. Armed with password cracking software, an intruder can discover a dictionary of the word password, or simple variation, in a matter of seconds. When you consider how much information is protected solely by passwords, it quickly becomes clear that good passwords are vital to preserving confidentiality.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 310 - 315 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Passwords must be protected against unauthorized disclosure, modification, & removal.

There are three types of attacks against passwords:

1. Password guessing
2. Password cracking
3. Password disclosure

Password Guessing:

Password guessing is guessing the password when a valid user ID is known. It can be done either manually or automatically, submitting the password of a particular user. For example, if the user ID is John attacker tries Jack and some other password until finds one or locked out. In any case, complex passwords provide protection against this type of attack.

Password Cracking:

Password cracking is done using a copy of the system file that stores account passwords in encrypted form. All current operating systems store passwords in an encrypted form by running the passwords through a one way hash. The hash is then stored, not the clear text password.

There are three types of cracking attacks:

1. Dictionary attacks
2. Brute force attacks
3. Hybrid attacks

1. Dictionary attacks:

If dictionary words are used as passwords, they can be readily broken, even when encrypted. That's because software has been created that gives the intruder the ability to take an entire dictionary's worth of words, run it through various encryption algorithms, and compare the results with the encrypted password file. If a match is found to the password hash, the cracker works backswords to discover what the password is. Simply put, dictionary words offer no protection at all as passwords. If you are thinking of using foreign words, forget it.

2. Brute force attacks:

A brute force attack tries every possible combination of letter, number, and punctuation value and format. A brute force attack will always succeed in cracking a password hash. However, depending on the strength of the password, the hashing formula, and the speed of the computer

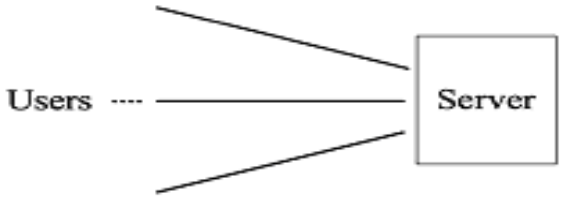
3. Hybrid attacks:

The Hybrid attackers build on the dictionary attacks by adding or substituting other characters or numbers for certain letters in dictionary words. Many people perform a simple substitution, or propend or append a character to a dictionary word to create a password.In Each time the user authentication is done by selecting a random number from the Quadratic residue set which is in turn form from random number that is chosen at each time of login life. Therefore, the intruder reaches different values each time which may take a long time for him to reach the value.

SYSTEM ANALYSIS:

Modal for Single Server:

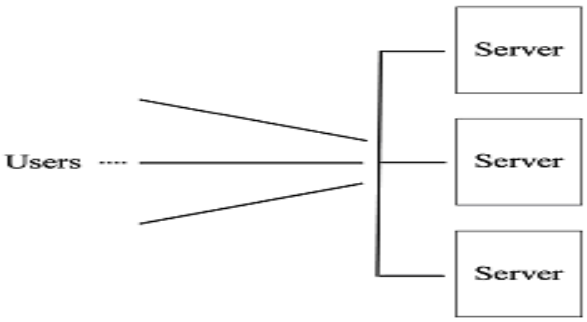
In Single server system, the user communicates with one server where the server validates against the password available in the central database and allows the user. But, this system has higher chance of attacks from intruders. The user authentication is done only by a single server which less secure than two server.



modal for single server

Modal for Multi-server:

Multi server systems client communicate with servers in parallel by establishing the connection with the servers. The users have to communicate with all the servers for the authentication simultaneously so there is demand on communication bandwidth and need for synchronization.



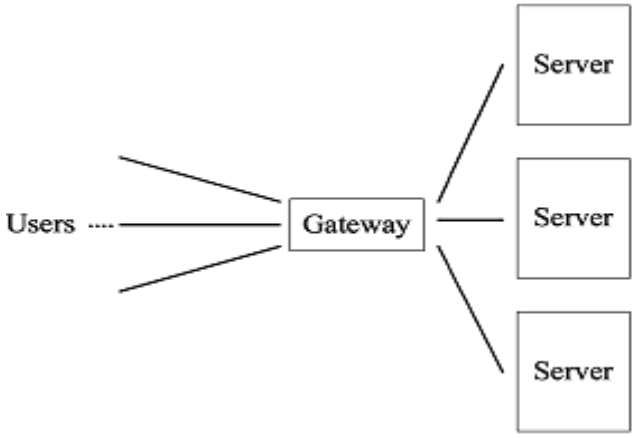
Multi-server model

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 310 - 315 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Modal for Gateway Multi-Server:

In the Gateway augmented multi server model, the gateway server is positioned between user and the multiple servers. The users have to communicate only with the gateway so it



Gateway multi-server model

removes the demand of simultaneous communications by user with multiple servers. There is an additional layer "gateway" in the architecture where gateway acts as rely messages between user and servers. It does similar to that of multi server.

Existing System:

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.

In addition, the server keeps track of the browser being used by the user and also the system related information. It the information does not match, 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.

BASIC PASSWORD AUTHENTICATION AND KEY EXCHANGE PROTOCOL

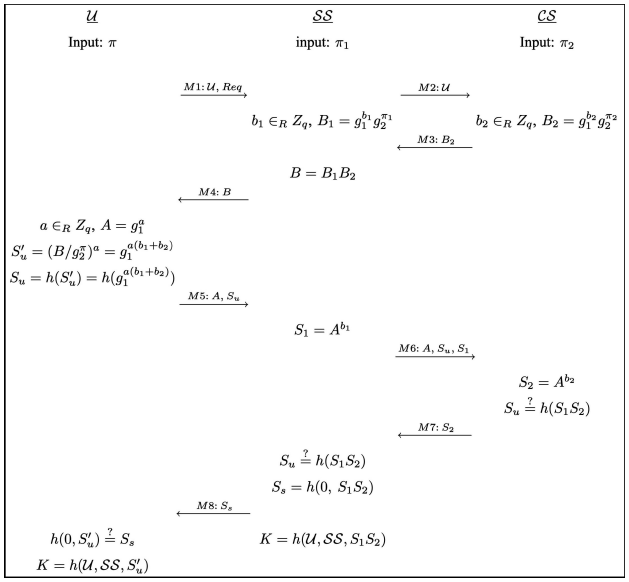
System Model

There are three entities those 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 t public server and the control server is away from the users. Users are not aware about the 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.

In Two server systems, the user is allowed to communicate with single system, public server where as the other system is the back end servers are 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.

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, 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.

Functional Requirements:

The project mainly contains the following modules

A. Client Registration

B. P A

C. Keys Exchange

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 310 - 315 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

D. Implementation for server

A. Client Registration:

User must be enters id and password to register into the database .after registering the user login into server using the registered id and password.

B. Password Authentication(PA):

Giving his id and password, password is send to the service server and to the service server collects the remaining password from the control to server and checks whether the user is valid or not.

C.Keys Exchange:

The user send to his password to the server and the service server divides the password into two steps , one step is send to the control server and remaining part is kept with the service server. The password is key exchanged between the two servers, if the password is valid the control server gives the authentication to the service server and then the service server provides the authentication to the user.

D.Implementation for Server :

this modules we will developed a service server to that interacts with the clients and will developed a control server will have the interaction with service server not with that clients.

User Registration

user must and should before hand register with the servers by establishing a shared password. The password π is divided as π_1 and π_2 the 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 *Server*1 in $M1$.

Basic Password Authentication Protocol The authentication and key Exchange between client and public server SS . the outline the basic password authentication protocols. The notations and symbols follows are tabulated in table .

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 $M2$. 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 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.

Proposed System

PROPOSED PASSWORD AUTHENTICATION AND KEY EXCHANGE PROTOCOL MODULE

Three entities those are involves in the system are the users, Service server(ss), and control server CS .

The services server is the public servers and the control server is the hidding end server in the two server model. In this protocol the users can only communicate with the public server and the control server is from the users. Users are not aware 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.

Proposed Password Authentication Protocol

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

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 310 - 315 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

enables between user and servers *Server*1 and *Server*2 . We outline the proposed password authentication protocol here. The user must be request after completing the user registration phase with *Server*1 or *Server*2 in message $M1$. If the user request *Server*1 , then *Server*1 computes the value of $f(x) = x^a \bmod n$, $U' = h(\prod_1)[f(x)]$ and $V' = h(\prod_1)[x]$. *Server*1 sends uid, U', V' to *Server*2 in $M2$.

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

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

$S_S = h(A^{b_1} S_2 \bmod p)$, 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 controlling server .
2. When the server is controlled by a passive adversary, the intruder may communicate 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 public server is unable to learn on either π or π_2 from the two pairs. The values that user and control server are replaced and passed to other so it is secured from offline dictionary attacks.

4.The protocol active outside adversary controlling no server.

CONCLUSION

The present authentication system should be used instead of existing server system as File Transfer Protocol and email servers where numbers of the users can increased by providing the two ways user authenticated 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.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 310 - 315 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

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 Key Exchange 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-Authenticateds Key Exchange Using Diffie-Hellman," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 156-171, 2000.

AUTHORS:

Anusha Thota received the B.Tech degree in Computer Science and Engineering and Technology from JNTU Kakinada in 2009 & pursuing her M.Tech in Software Engineering from JNTU Kakinada

S.Amarnath Babu is presently working as Associate Professor Dept of Computer Science and Engineering in St.Ann's College of Engineering and Technology, Chirala. He received the B.Tech degree from Acharya Nagarjuna Bapatla, and M.Tech in JNTU Hyderabad. He has more than 11years of Excellence in Teaching Experience.He Published 6 Conferences and 5 journals.

.