ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Multi Server Password Authentication by Key Exchange Protocol in Secure Manner

S.A.Deshpande[1], Pawar Vishal[2], Rane Ashwini[3], Gite Supriya[4]

Assistant Professor, IT Department, PVG's COET, Pune, India[1]

Student, IT Department, PVT's COET, Pune, India[2,3,4]

Abstract: Client and a server share a password using Password-authenticated key exchange (PAKE) to authenticate each other and establish a cryptographic key by exchanging previously generated shares. In this scenario, all the passwords are stored in a single server which will authenticate the client. If the server is hacked, for example, hacking or even insider attack, passwords stored in database will become publicly known. In this paper, we consider a setting where two servers are used to authenticate a client and if one server is compromised, the attacker still cannot be able to view the client's information from the compromised server. In this paper we are going to provide the system which uses the El-gamal encryption and collectively AES (Advance encryption standard) algorithm. And also uses the Diffee-hellman for key exchange. In this paper, we are going to provide the solution for SQL_INJECTION attack which is commonly happens on the database. The proposed scheme is a password-only system in the sense that it requires no public key cryptosystem and, no PKI. In the given authentication schema we also use SMS integration API for two step verification like Gmail, it will provide the additional security to end user.

Keywords: Diffie-Hellman key exchange, El-gamal encryption, AES algorithm, SQL_INJECTION attack.

I. INTRODUCTION

Passwords are the most common way to prove identity of user when accessing protected data, accounts and your computer itself (via User Accounts). The use of strong passwords is therefore essential in order to protect your security and identity. The best security in the world is useless if a malicious person has a legitimate user name and password. A password is a secret word or set or collection of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from unauthorized person. Unfortunately, many security systems are designed such that security relies entirely on a secret password. Many researchers show that people pick easy to guess passwords. For example, an early study on password security found that over 15% of users picked passwords shorter or equal to three characters.

Furthermore, they found that 85% of all passwords could be trivially broken through a simple exhaustive search to find short passwords and by using a dictionary to find longer ones. Now a day every important transaction requires the password. So it is required to keep track of password in the database. So, the security of password is important concern. Therefore it is highly required to preserve the password from every attacker. Previously password-based authentication systems transmitted a cryptographic hash of the password over a public channel so when attacker hacks the database with the help of public key he may get required passwords otherwise the attacker can work online, rapidly testing possible passwords against the true passwords hash value. Studies have consistently shown that a large fraction of user-chosen passwords are readily guessed automatically.

Recent research advances in password-based authentication have allowed a client and a server mutually to authenticate with a password and meanwhile to establish a cryptographic key for secure communications after authentication. The current solutions for password based authentication follow two strategies. In first strategy, assumes that the client keeps the servers public key in addition to share a password with the server. In this paper, the client can send the password to the server by public key encryption. The second strategy is called password-only strategy which introduces a set of so-called encrypted key exchange protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose.

Previous protocols for password-based authentication assume a single server stores all the passwords necessary to authenticate clients. So, when the attacker attacks the server, the whole meaningful information regarding password will be available to attacker in encrypted form and with the use of some encryption tool and guessing ,the attacker can decode the required password and can access the system information. So to avoid such a problem we are giving solution of efficient two server password authentication system with two step mobile verification. In this system, user is secured by using two servers password authentication process along with proper mobile verification. When user enters the password, it will be forwarded to web server using SOAP (Simple Object Access Protocol). SOAP is a secure protocol which is used to hold and sends entered password to web server. At web Server the password is encrypted using Diffee-hellman key exchange protocol and ElGamal encryption scheme as described below. After encryption at web server the

DOI 10.17148/IJARCCE.2015.4433

encrypted characters are divided by total no. of servers i.e. if C is a cipher text from password plain text P and N is no. of servers where passwords will be stored then each server (Si) will get Si = C=N

It means, If no. of servers where we are storing password is two and the count of cipher text character is 10 then every server will be storing 5 Cipher text characters.
For example, if pwd1 is a data stored in server1 say S1 and pwd2 is a data stored in server2 say S2 then the whole cipher text C is obtained as C = pwd1 + pwd2

So, when attacker attacks the server, he able to get insufficient encrypted information. Therefore whole password cannot be disclosed. Although we use the concept of public key cryptosystem, our protocol follows the password-only model. The encryption and decryption key pairs for the two servers are generated by the client and delivered to the servers through different secure channels during the client registration, as the client in any two-server PAKE protocol sends two halves of the password to the two servers in secret, respectively. In fact, a server should not know the encryption key of another server and is restricted to operate on the encryption of the password on the basis of the homomorphic properties of ElGamal encryption scheme. Along with this when data is forwarded to web server from client side, the web server will generate a unique identification number which will be forwarded to users registered Mobile Number. User can access his data only when entered unique identification number matches with web servers unique identification Number for further processing. This system can be applied in distributed systems where multiple servers exist. In all existing two-server PAKE protocols, two servers are provided random password shares p1 and p2 subject to p1+ p2=p. In our protocol, we gives the password share to one server S1 with an encryption

$$(g_2^{P};Pk_2) \tag{1}$$

and another server S2 with an encryption

$$(g_2^{P};Pk_1) \tag{2}$$

Where, pk_1 and pk_2 are the encryption keys of S1 and S2 respectively. In addition, two servers are gives random password shares b1 and b2 where,

$$b_1b2=H(p) \tag{3}$$

where H is a cryptographic hash function. Hence the password p is undisclosed unless the two servers compromise.

Although we use the concept of public key cryptography system, our protocol follows the password-only model. The encoding and decoding key pairs for the two servers are establish by the client and provided to the servers via different secure channels while the client registration, as the client in any two-server PAKE protocol sends two parts of the password to the two servers in secure manner, respectively. But, a server should not know the encoded key of another server this is the homomorphic properties of El-Gamal encryption scheme. For example, given

$$(g_2^{p};Pk_2) \tag{4}$$

S1 can construct

$$(Ag_2^{p};\ Pk_{2)}\text{and}(g_2^{(a:p)};Pk_2) \tag{5}$$

for any group element A and integer a without the knowledge of the encryption key pk2.

II. RELATED WORK

A. Katz et.al system

In 2005, Katz et al. proposed the two-server password only authenticated key exchange protocol in context of security standard model. In their setting, client C can choose any random password and accordingly server A and B generate the password shares P1 and P2 where P=P1+P2. KOY's protocol execute twice in their setting, one between the client C and the server A, by using the server B to provide authentication, and one between the client C and the server B, using the server A to provide the authentication. The evolvement of the other server is mandatory since the password is break into two servers. At the end of the execution each server and the client agree on a secret session. The advantage of this protocol structure is to supports two servers to compute in parallel but it failed for practical use.

B. Yang et al. system

According to Brainard et al.s work in 2005, Yang et al. proposed an asymmetric setting, where a one server is called as service server (SS) which interacts with the client, while a other 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 issues a request, and SS responds with B=B1 B2, where

$$B_1=g1^{(b1)}g2^{(\pi1)} \tag{6}$$

And

$$B_2=g1^{(b2)}g2^{(\pi2)} \tag{7}$$

are generated by SS and CS on the basis of their random password shares 1 and 2, respectively and then the client can obtain

$$g1^{(b1+b2)} \tag{8}$$

by eliminating the password

$$\pi=\pi1+\pi2 \tag{9}$$

from B, i.e. computing

$$B=g2 \tag{10}$$

Next, SS and the client authenticate each other by checking if they can agree on the same secret session key, either

$$g1^{a(b1+b2)} \tag{11}$$

OR

$$g1^{(aa1(b1+b2))} \tag{12}$$

C. Jin Two-Server System

In 2007,yang protocol required maximum communication rounds between SS and CS, this drawback is removed by the jins protocol by adding the necessary advancement

$$B=g1^{a2} \quad (13)$$

to SS; SS forwards

$$B_1=B/g_1^{b1}g_2^{\pi 1} \quad (14)$$

to CS; CS returns

$$A_{1=}g_1^{b2}; B_2 = ((b1_{=g2}^{(2)}))^{(b2)}{}_{=\ g1}{}^{((a-\ b1)b2} \quad (15)$$

to SS; SS computes

$$B2{}_{=\ ((B2=A\ 1}{}^{(\ b2))}{}_{)}{}^{(b}3^{)}{}_{=\ g}{}^{(ab}2^{b}3^{)} \quad (16)$$

and responds

$$A_2 = A_1^{(\ b3)}; S_1 = H(B_3) \quad (17)$$

to the client, where H is a hash function. Next, SS and the client authenticate each other by checking if they agree on the same secret session

$$g_1^{(ab}2^{b}3^{)} \quad (18)$$

where a,(b1, b3), b2 are randomly selected by the client, SS and CS, respectively.

III. LITERATURE SURVEY

1) In 2005, Katz et al. [2] proposed the _rst 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 [3] 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 [3], 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 et al.s protocol [2] is symmetric where two servers equally contribute to the client authentication and key exchange. For their basic protocol secure against a passive adversary, each party performs roughly twice the amount of works as the KOY [3] protocol. For the protocol secure against active adversaries, the work of the client remains the same but the work of the servers increase by a factor of roughly 2-4. This is the protocol structure which supports two servers to compute in parallel. Inefficiency for practical use.
2) Built on Brainerd et al.[9] work in 2005, Yang et al. [5] suggested an asymmetric setting, where a front-end 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 [5] and several asymmetric password-only two-server PAKE protocols [6], [7] 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 et al.s 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 et al.s protocols are more efficient than Katz et al.s protocols in terms of communication and computation complexities, Its protocol structure which requires two servers to compute in series and needs more communication rounds.
3) In 2007, Jin [7] further improved Yang et al.s [5] protocol and proposed a two-server PAKE protocol with less communication rounds. In their protocol, the client sends

B = g1ag2 to SS; SS
forwards
B1 = B=g1(b1)g2(1) to CS;

CS returns
A1 = g1(b2); B2 = B1=g2(2))(b2) = g1((a-b1)b2)toSS;
SS computes
B3 = (B2=A1(b2))(b3) = g(a(b2)(b3))
and responds
A2 = A1(b3); S1 = H(B3) to

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 et al.s protocol without introducing additional computation complexity. Its protocol structure which requires two servers to compute in series.

IV. PROPOSED WORK

In this paper, we propose a new symmetric solution for two-server PAKE. In all existing two-server PAKE protocols, two servers are provided random password shares pw1 and pw2 subject to pw1 + pw2 = pw. The system we are going to developed is capable to remove the disadvantages of existing system and produced the more efficient system. Our protocol can be applied in distributed systems where multiple servers exist. For example, Microsoft active directory domain service (ADDS) is the foundation for distributed networks built on Windows server operating systems that use domain controllers. AD DS provides structured and hierarchical data storage for objects in a network such as users, computers, printers, and services.AD DS also provides support for locating and working with these objects. For a large enterprise running

DOI 10.17148/IJARCCE.2015.4433

its own domain, there must be two AD DS domain controllers, for fault-tolerance purpose. To authenticate a user on a network, the user usually needs to provide his/her identification and password to one AD DS domain controller. Based on our two-server PAKE protocol, we can split the users password into two parts and store them, respectively, on the two AD DS domain controllers, which can then cooperate to authenticate the user. Even if one domain controller is compromised, the system can still work. In this way, we can achieve more secure AD DS. The remainder of this project is organized as follows: two cryptographic building blocks of our protocol, Diffee-Hellman key exchange protocol and El-Gamal encryption scheme and two-server PAKE protocol.

Our Protocol Works in Four Phases:

A. Initialization

To secure hash function

H : 0; 1!Zq

the two servers S1 and S2 jointly decide a cyclic group G of large prime order q with a generator g1 which maps a message of random length into an l-bit integer, where l=log2q. After that,S1 chooses an integer s1 from Z*q randomly, and S2 chooses an integer s2 from Z*q randomly, and S1 and S2 exchange g1s1 and g1s2 . Next, S1 and S2 together publish public system parameters G,q, g1,g2,H where g2 = g1s1s2 :

B. Registration

For authentication, each client C is need to register both server S1 and S2 through unlike secure channels. Firstly, the client C generates encryption and decryption key pairs (xi; yi) using the public parameters published by the two servers where yi = g1xi for the server Si (i=1).

After that, client C elects a password pwC and encrypts that password by using the encryption key yi, i.e.,(g2pwc; yi) = (Ai;Bi) = (g1ai; g2pwcyiai) (i=1,2) where ai is chosen randomly from Z _ q , according to El-Gamal encryption. After that, the client C chooses b1 randomly from Z*q and lets b2 = H(pwC) b1, where stands for two l-bit blocks exclusive OR Finally, client C sends the password authentication information to S1 through a secure channel, i.e. Authc(1) = x1; a1; b1; (g2pwc; y2) and the password authentication information to S2 through another secure channel i.e. Authc(2) = x2; a2; b2; (g2pwc; y1):

Next, client C remembers the only password pwC.

C. Authentication and Key Exchange

Now we consider that the two servers S1 and S2 having the authentication information of a client C, to authenticate the client C there are five steps for the S1 and S2 and establish private session keys with the client C in terms of parallel computation. That we will discussed later.

D. Two step Mobile Verification

In that phase finally we will generate OTP or server generated signature for drastic supervision using SMS API integration.

V. SYSTEM ARCHITECTURE

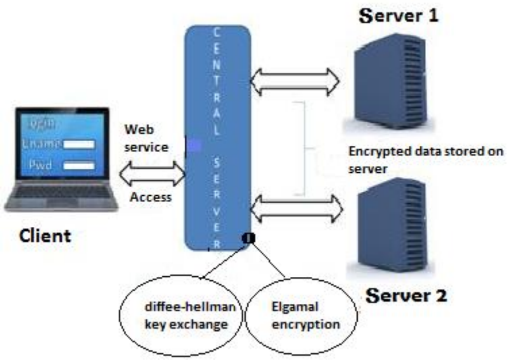

Fig: Two server system architecture

System architecture or system's architecture is the conceptual model that defines the structure, behaviour, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures of the system.

A. Client Registration Module

In this module client is registering himself as an authentic user by entering username, password, personal mobile number and other necessary information. The entered data will be directed towards web server using SOAP protocol for further processing.

B. Web Service Operations

In this module the incoming password information is encrypted using Diffee-Hellman Key Exchange Protocol and ElGamal Encryption Scheme. After encryption encrypted password is broken into two sub passwords on the basis of length of total password i.e. if length of encrypted password is 10 characters then each sub password contain 5 characters. All the sub passwords will be directed and stored in two different servers.

C. Server Modules (Two Server)

This module will store the password coming from web server and will be retrieved only at the time of authentication to maintain the securities in the system.

VI. OUR MODULES

A. User Registration Module

In the given module all users can create his own profile, there are few mandatory details with validations, First user will fill his appropriate details like name, address, username, password etc. All the things will give the user type and identity of user. Finally user submits all details.

Input: User Details.

Output: Message for profile is creating.

B. Service Invocation Module

In that module when user will click on registration button and give request for create a profile then service will be invoked. The central service having the logic to take input from user GUI then converts it encrypted format like plain text to cipher text using El-gamal Encryption and then

DOI 10.17148/IJARCCE.2015.4433

maintain the replica on how much servers are available are there in different data pieces. Input: Collect Data which fill by user. Output: Encrypted data successfully and profile created successfully.

C. User Request Module

After creation the profile, whenever same user will give the request for login with the system, it will again forward to centralized service system. Before checking the identity of user system will take all inputs and store in virtual data tables.
Input: User login Details with user type.
Output: Please wait system is verifying.

D. User Authentication Module

Here system having all details of user likes username and password. Now here system will call both data servers and take the encrypted data paces, then apply the same algorithm but here is reverse process known as decryption. The decrypted data will be match with user password we already store in virtual data table then user will be authenticated.
Input: User login details.
Output: User login success or login failed.

E. Two Step Verification Module

After verifying both servers we will add another security schema for drastic security. Two step verification give the assurance given user is trustworthy user. In that phase after verifying both server system will generate random key and send in user cell phone which is given by user at the time of registration, then system will be ask for verify the code. If the system code and user entered code is correct then it will given the next access of system and the user recognized as authenticate user.
Input: Secrete code receive on mobile.
Output: Authentication Success or you have enter wrong code.

VII. CONCLUSION

Overall, the project design will achieve its objectives. It is Efficient for practical use. The project will provide an efficient, meaningful and secure two server password authentication system along with mobile based validation system for only authentic user access. Yang et al .s protocols are more efficient than Katz et al .s protocols in terms of communication and computation complexities. It is more secure rather than all existing cryptography algorithm. To insert users precise information such as password we use SOAP protocol. To configure the SOAP we use web services.

ACKNOWLEDEMENT

We take this opportunity to thank our guide **Prof. S.A.Deshpande** for their valuable guidance, timely support and Inspiration. We also thankful to Head of the Department **Prof. Mr. .G.V. Garje** for providing all the necessary facilities, which were indispensable in the completion of this paper. We are also thankful to all the staff members of the Department of Information Technology of Pune Vidyarthi Griha's College of Engineering and Technology, Pune for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

[1]. M. Abdalla and D. Pointcheval, Simple Password-Based Encrypted Key Exchange Protocols, Proc. Intl Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.
[2]. J. Katz, P. MacKenzie, G. Taban, and V. Gligor, 'Two Server Password-Only Authenticated Key Exchange,' Proc. Applied Cryptography and Network Security (ACNS 05), pp. 1-16, 2005.
[3]. J. Katz, R. Ostrovsky, and M. Yung, E_cient Password-Authenticated Key Exchange Using Human-Memorable Passwords,Proc. Int l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (Eurocrypt 01), pp. 457-494,2001.
[4]. W. Ford and B.S. Kaliski Jr., Server-Assisted Generation of a Strong Secret from a Password, Proc. IEEE Ninth Intl Workshop Enabling Technologies: Infrastructure for Collaborative Enter-prises, pp. 176-180, 2000.
[5]. Y. Yang, F. Bao, and R.H. Deng, A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprise, Proc. 20th IFIP Intl Information Security Conf. (SEC05), pp. 95-111, 2005.
[6]. S. Halevi and H. Krawczyk, Public-Key Cryptography and Password Protocols, ACM Trans. Information and System Security, vol2, no3, pp 230-268, 1999.
[7]. H. Jin, D.S. Wong, and Y. Xu, An E_cient Password-Only Two-Server Authenticated Key Exchange System, Proc. Ninth Intl Conf. Information and Comm. Security (ICICS 07), pp. 44-56,2007.
[8]. D.Jablon,Password Authentication Using Multiple Servers, Proc. Conf. Topics in Cryptology.The Cryptographers Track at RSA,pp.344-360, 2001.
[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.

BIOGRAPHIES

Pawar Vishal Wamanrao Student of Information Technology Department, Pune Vidyarthi Griha’s College Of Engineering And Technology, Pune.

Rane Ashwini Dhananjay Student of Information Technology Department, Pune Vidyarthi Griha’s College Of Engineering And Technology, Pune.

Gite Supriya Subhash Student of Information Technology Department, Pune Vidyarthi Griha’s College Of Engineering And Technology, Pune.

DOI 10.17148/IJARCCE.2015.4433