International Journal for Rapid Research in Engineering Technology and Applied Science
ISSN (Online): 2455-4723
Vol 1 Issue 1 December 2015

Two Server Password Only Authentication Key Exchange through Web Service

Mrunal R Nikam*, Prof. Chhaya Nayak**
IInd Year Mtech, Department of Computer Science and Engineering, Indore, MP, India*
HOD, Department of Computer Science and Engineering, Indore, MP, India**
*nikam.mrunal@yahoo.com**, *hod.computers@bmcollege.ac.in***

Abstract: A PAKE protocol is a cryptographic protocol that allows two parties one as client and second as server, to mutually authenticate each other by sharing the knowledge of password and establish cryptographic keys BY exchanging messages and without explicitly revealing the password. In General the practice is to store the password or authentication information on single server belonging to client. If such a server gets compromised then there is a risk factor associated, which causes a large number of client's passwords to get exposed. In such scenarios, the solution to verify a password is to split it among two or more servers even if one of the server gets compromised still there is chance for recovery. In this proposed work, we will be implementing a symmetric solution for two-server PAKE, where a registered user i.e. client and its related information i.e. username & password will be given to web server using web services where it will be encrypted using Diffie-Hellman key exchange and ElGamal encryption algorithm and a public key is generated which will be given to client for decryption process. The encrypted data is broken & distributed among no. of active servers of system which will be united if & only if trusted user is accessing the account. The system is integrated with two step mobile based verification system based on random number for authenticating user's mobile.

Keywords: Diffie-Hellman, ElGamal Encryption, Web Service, PAKE, SOAP.

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. 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 offline, rapidly testing possible passwords against the true password's 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 server's public key in addition to share a password with the server. In this setting, 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 & 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 Only Authentication Key Exchange through Web Service". In this system, user is secured by using two server's password authentication process along with proper mobile verification. Proposed System will involve the use of Updated Diffie Hellman, Updated ElGamal Encryption and web-service.

The two-server model comprises two servers at the server side, one of which is a public server exposing itself to users and the other of which is a back-end server staying behind the scene; users contact only the public server, but the two servers work together to authenticate users.

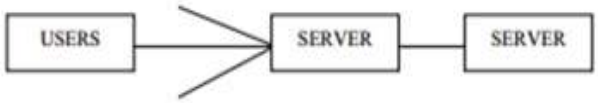

Figure 1: Two Server Model

II. Literature Survey

Katz et.al system: In 2005, Katz et al. [2] 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 [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 pw1and pw2 subject to pw = +.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 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 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.
Advantage: - The advantage of Katz et al.'s protocols is the protocol structure which supports two servers to compute in parallel.
Disadvantage: - Inefficiency for practical use

Yang et al. System: Built on Brainard et al.[4] 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=, where = and = are generated by SS and CS on the basis of their random password shares π1 and π2, respectively and then the client can obtain by eliminating the password π(=π1+π2) from B, i.e. computing B/. Next, SS and the client authenticate each other by checking if they can agree on the same secret session key, eitheror ,with the help of CS, where a, (,) and 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.

Advantage:-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,
Disadvantage:-it's protocol structure which requires two servers to compute in series and needs more communication rounds.

Jin Two-Server System: In 2007, Jin further improved Yang et al.'s [8] protocol and proposed a two-server PAKE protocol with less communication rounds. In their protocol, the client sends B= to SS; SS forwards = B/ to CS; CS returns =, = =to SS; SS computes ==and responds =, =H () 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 ,where a,(,), are randomly chosen by the client, SS and CS, respectively.
Advantage: -It needs less communication rounds than Yang et al.'s protocol without introducing additional computation complexity.
Disadvantage:-Its protocol structure which requires two servers to compute in series.

Xun-Ling-Wang System: In 2014 , Xun ,Ling ,Wang proposed PAKE protocol 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 paper, a scenario is considered where two servers cooperate to authenticate a client and if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server.
Advantage: - protocol runs in parallel and is more efficient than existing symmetric two-server PAKE protocol, and even more efficient than existing asymmetric two-server PAKE protocols in terms of parallel computation.
Disadvantage: - Needs more Computational rounds.

III. Protocols

A. Diffie-Hellman Key Exchange Protocol

Diffie Hellman establishes a shared secret that can be used for secret communications while exchanging data over a public network. To implement Diffie-Hellman[3], the two end users Alice and Bob, at the same time as communicating under a channel they mutually agree on two positive whole numbers q and g, such that q is a prime number and g is a

generator of q. The generator g is a number to facilitate, when raised to constructive whole-number powers less than q, never produces the same result for any two such whole numbers. The value of q may be large but the value of g is usually small. Diffie Hellman key exchange (DH)[nb 1] is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. Although Diffie Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).The method was followed shortly afterwards by RSA, an implementation of public key cryptography using asymmetric algorithms.Once Alice and Bob have agreed on q and g in private, they choose random positive whole-number m and n, Next, Alice and Bob compute public keys A and B based on their personal keys according to the formulas

1. $A = g^m \bmod p$
2. $B = g^n \bmod q$
3. The two users can share their public keys A and B over a communications medium assumed to be not confident, such as the Internet or a commercial wide area network (WAN). From these public keys, a number x can be generated by either user on the basis of their own personal keys. Alice computes K1 using the formula
4. $K1 = (B)^m \bmod q$
5.Bob computes K2 using the formula
6.$K2 = (A)^n \bmod q$

Obviously K1=K2.So this will be shared secret key among Alice and Bob.

B. ElGamal Encryption Scheme

In cryptography, the ElGamal encryption system [5] is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie Hellman key exchange. It was described by Taher Elgamal in 1984. It consists of key creation, encryption, and decryption all the steps (Algorithms) as followsKey generation:- The key generator works as follows: 1. Alice generates an efficient description of a multiplicative cyclic group G of order q with generator g. See below for a discussion on the required properties of this group. 2. Alice chooses a random x from 1, q-1. 3. Alice computes h = gx: 4. Alice publishes h, along with the description of G,q,g as her public key. Alice retains x as her private key which must be kept secret.

IV. Web-Service

A Web service, in the context of .NET, is a component that resides on a Web server and provides information and services to other network applications using standard Web protocols such as HTTP and Simple Object Access Protocol (SOAP).A Web service is a method of communication between two electronic devices over World Wide Web (WWW). A web service is a software task provide at a network address over the web or the cloud; it is a service that is"always on" as in the concept of utility computing.

What is SOAP?

- SOAP is a communication protocol SOAP is for communication between applications
- SOAP is a format for sending messages .
- SOAP communicates via Internet
- SOAP is platform independent SOAP is language independent SOAP is based on XML
- SOAP is simple and extensible
- SOAP allow you to get approximately firewalls
- SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.

V. Proposed System

The proposed work is based on two servers Model as shown in Figure 1 where even if one server gets compromised still hacker can't get into the system and this goal will be achieved with the help of Updated Diffie Hellman and Updated ElGamal Encryption and Web Service .Our Proposed System works in following stages

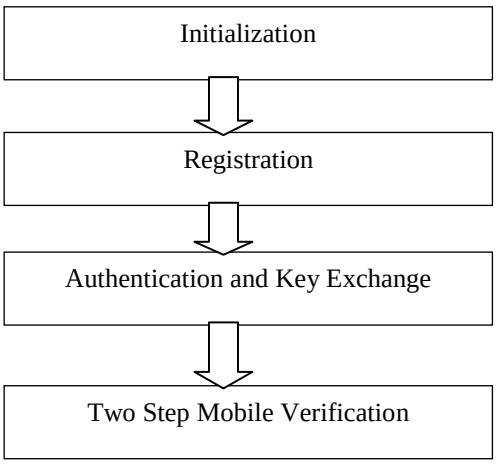

Figure 2: Methodology Block Diagram

Initialization: In this Stage we generate two keys for two different servers, which includes a long process to create two different keys like a prime number, secret numbers of both servers etc. then both the servers will exchange their generated keys with each other and when both generated final keys are same for both the servers then both servers are validated with each other. The system uses modified Diffie Hellman key exchange protocol for this stage

Registration: In this stage the new user will get registered on both the server s with all the validations and when once a password has been entered by user then with the help of Updated ElGamal Encryption 2 ciphertext will be generated and will be stored with the help of web service with all other parameters on both the servers.

Authentication and Key Exchange: Using combination of Updated Diffie-Hellman Key Exchange Protocol and Updated Elgamal Encryption the authentication to the user will be provided by encryption and decryption method.Web Service plays a middleware role in this stage between client and two servers for authenticating the user.

Two Step Mobile Verification: In this when user will enter his / her password then a code will send to user mobile and then if the code enter by user and code the system is having gets match then only user will login i.e. strong security is provided.

A. Proposed System Architecture

A 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. The figure depicts the architecture and contains client, 2 serves, central server for web service and cooperting algorithms.

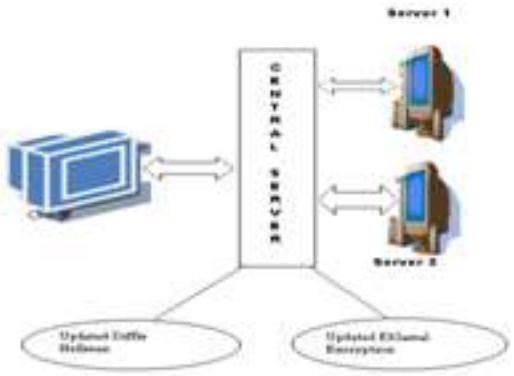

Figure 3: Proposed System Architecture

B. Proposed Algorithms

Proposed Updated Diffie Hellman Algorithm

Here two end users Alice and Bob, while communicating over a channel they mutually agree on two positive whole numbers q and g, such that q is a prime number and g is a generator of q. The generator g is a number that, when raised to positive whole-number powers less than q, never produces the same result for any two such whole numbers. The value of q may be large but the value of g is usually small.Once Alice and Bob have agreed on q and g in private, they choose random positive whole-number m and n, Next, Alice and Bob compute public keys A and B based on their personal keys according to the formulas.

1) A and B compute the key ans
2) Generate the prime number from large cyclic order P
3) Both will select a number between 2 to P-1 is g
4) A and B both select individual secrete number as a and b
5) A calculate Resa=g.modpow(a,p)
6) B calculates Resb=g.modpow(b,p)
7) Then A sends Resa to B and B sends Resb to A
Finally both calculate the final key
finalkeyA=Resb.modpow(a,p)
finalkeyb=Resa.modpow(b,p)
if(finalkeyA==finalkeyb)
Server Authenticetd
Else Server authentication fail

Proposed Updated ElGamal Encryption

It consists of key generation, encryption, and decryption algorithms as follows:

Key generation

1) Alice generates an efficient description of a multiplicative cyclic group G of order q with generator g. See below for a discussion on the required properties of this group.
2) Alice chooses a random x from {1, …, q-1}.
3) Alice computes $h = g^x$.
4) Alice publishes h, along with the description of G,q,g as her public key. Alice retains x as her private key which must be kept secret.

Encryption

The following is the encryption algorithm to encrypt a message *m* to Alice under her public key *(G, g, q, h)*

1. Bob chooses a random y from {1, …, q-1}, then calculates $c_1 = g^y$.
2. Bob calculates the shared secret *s*= h^y.
3. Bob converts his secret message into an element m' of *G*.
4. Bob calculates. $c_2 = m'$.s
5. Bob sends the cipher text (c_1, c_2) = ($g^y, m', (g^x)^y$) to Alice.

Decryption

The following is the decryption algorithm to decrypt a cipher text (c_1, c_2) with her private key *x*
1) Alice calculates the shared secret s= c_1^x
2) And then computes $m' = c_2 . s^{-1}$ which she then converts back into the plaintext message m, where s^{-1} inverse of sin the group *G*.

The decryption algorithm produces the intended message, since
$c_2 . s^{-1} = m' . h^y . (g^{xy})^{-1} = m' . g^{xy} . g^{-xy} = m'$.

VI. Conclusion

- In this system, 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.
- Performance analysis has shown that our protocol is more efficient than existing system.

References

[1] Pawani Porambage, Corinna Schmitty, Pardeep Kumar, Two-Phase Authentication Protocol For Wireless Sensor Networks In Distributed Iot Applications, Ieee 2014.
[2] Basel Alomair, Radha Poovendran, Senior Member, Efficient Authentication For Mobile And Pervasive Computing, IEEE , Transaction Paper.
[3] Xun Yi, San Ling And Huaxiong Wang, Efficient Two- Server Password Only Authenticated Key Exchange, IEEE 2013, Transaction Paper.
[4] S. Bellovin And M. Merritt, Encrypted Key Exchange: Password-Based Protocol Secure Against Dictionary Attack, Proc. IEEE Symp. Research In Security And Privacy, Pp. 72-84, 1992.
[5] 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.
[6] 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.
[7] 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 Enterprises, Pp. 176-180, 2000.
[8] 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.
[9] 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.
[10] Jablon, Password Authentication Using Multiple Servers, Proc. Conf. Topics In Cryptology: The Cryptographers Track At RSA (RSA-CT 01), Pp. 344-360, 2001.
[11] H. Jin, D.S. Wong, And Y. Xu, An Efficient Password-Only Two- Server Authenticated Key Exchange System, Proc. Ninth Intl Conf. Information And Comm. Security (ICICS 07), Pp. 44-56, 2007.
[12] J. Katz, R. Ostrovsky, And M. Yung, Efficient Password- Authenticated Key Exchange Using

Human-Memorable Passwords, Proc. Intl Conf. Theory And Application Of Cryptographic Techniques: Advances In Cryptology (Eurocrypt 01), Pp. 457-494, 2001.

[13] J. Katz, P. Mackenzie, G. Taban, And V. Gligor, Two-Server Password-Only Authenticatedkey Exchange, Proc. Applied Cryptography And Network Security (ACNS 05), Pp. 1-16, 2005.

[14] 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.

[15] M. Abdalla, O. Chevassut, And D. Pointcheval, "One-Time Verifier-Based Encrypted Key Exchange," Proc. Eighth Int'l Conf. Theory And Practice In Public Key Cryptography (PKC '05), Pp. 47-64, 2005.

[16] 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.

[17] Boneh And M. Franklin, "Identity Based Encryption From The Weil Pairing," SIAM J. Computing, Vol. 32, No. 3, Pp. 586-615, 2003.

[18] Boneh, "The Decisional Diffie-Hellman Problem," Proc. Third Int'l Algorithmic Number Theory Symp., Pp. 241-250, 1998.

[19] 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.

[20] W. Diffie And M.E. Hellman, "New Directions In Cryptography," IEEE Trans. Information Theory, IT-22, No. 6, Pp. 644-654, Nov. 1976.

[21] 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.

[22] T.M.A. Lomas, L. Gong, J.H. Saltzer, And R.M. Needham, "Reducing Risks From Poorly-Chosen Keys," ACM Operating Systems Rev., Vol. 23, No. 5, Pp. 14-18, 1989.

[23] 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 In Cryptology (Asiacrypt '00), Pp. 599-613, 2000.

[24] R. Rivest, A. Shamir, And L. Adleman, "A Method For Obtaining Digital Signatures And Public-Key Cryptosystems," Comm. ACM, Vol. 21, No. 2, Pp. 120-126, 1978.

[25] M. Szydlo And B. Kaliski, "Proofs For Two-Server Password Authentication," Proc. Int'l Conf. Topics In Cryptology (RSA-CT '05),Pp. 227-244, 2005.

[26] Y. Tsiounis And M. Yung, "On The Security Of Elgamal Based Encryption," Proc. First Int'l Workshop Practice And Theory In Public Key Cryptography: Public Key Cryptography (PKC '98), Pp. 117-134, 1998.

[27] 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.

[28] Y. Yang, R.H. Deng, And F. Bao, "A Practical Password-Based Two-Server Authentication And Key Exchange System," IEEE Trans. Dependable And Secure Computing, Vol. 3, No. 2, Pp. 105-114, Apr.-June 2006.

[29] 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.

[30] X. Yi, R. Tso, And E. Okamoto, "ID-Based Group Password-Authenticated Key Exchange," Proc. Fourth Int'l Workshop Security: Advances In Information And Computer Security (IWSEC '09), Pp. 192-211, 2009.

[31] X. Yi, R. Tso, And E. Okamoto, "Three-Party Password-Authenticated Key Exchange Without Random Oracles," Proc. Int'l Conf. Security And Cryptography (SECRYPT '11), Pp. 15-24, 2011.

[32] X. Yi, R. Tso, And E. Okamoto, "Identity-Based Password-Authenticated Key Exchange For Client/Server Model," Proc. Int'l Conf. Security And Cryptography (SECRYPT '12), Pp. 45-54, 2012.