Asian Journal of Computer Science and Technology (AJCST)
Vol.2.No.2 2014 pp 15-18.
available at: www.goniv.com
Paper Received :05-03-2014
Paper Published:28-03-2014
Paper Reviewed by: 1. John Arhter 2. Hendry Goyal
Editor : Prof. P.Muthukumar

IMPROVING SERVICE CREDIBILITY IN PASSWORD AUTHENTICATED PEER SERVICES

S.Pavithra, **E.Yuvabharathi**
Chennai Institute of Technology,
Kanchipuram District, Kundrathur-600069.

ABSTRACT

Two server secret word-based authentication protocols(Two-Server PAKE), where two servers co-operate to authenticate a client on the basis of secret word only and if one server is compromised due to denial of service attack (DDOS), the attacker still cannot make believe to be the client with information from the compromised server. New research advances in secret word based authentication and follow two models. The initial model, called Public key infrastructure suggests, that the client having the server's public key in additional to share a secret word to the server. In this setup, the client has to send the secret word only to the server by public key encryption (PKE). The next model is called secret word-only model which follows encrypted key exchange (EKE) protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose. A secret word-only authentication protocol which is both convenient and provably secure identify with cryptographic assumption. Our protocol is symmetric and, can run in similar to establish secret session keys between the client and peer servers, respectively. In case any one of the two peer servers shuts down due to the Distributed Denial-of service attack (DDOS), other server can proceed to provide ceremony to valid clients. In case of similar computation and reliable service, a symmetrical protocol is superior to an asymmetrical protocol.

Index Terms- Two server PAKE, DDOS, PKE, EKE, public key infrastructure, Diffie-Hellman, ElGamal encryption, symmetrical protocol.

1. INTRODUCTION

Nowadays, password used for user authentication to prove identity or access approval to a resource, it should be kept secret from the authorized people or attacker. Recent times, the username and password which means the logging process that controls the access to the protected computer operating system, cable TV, mobile phones, retrieving e-mail, database, networks, web sites, banking transactions and many other. Password must be selected such that it must be secure and memorable and should not be easily guessed by attacker. Secret word should not stored directed into database, in case if any attacker gains the authority to access means then definitely there will be loss in the information. In the proposed secret word authenticated services, to authenticate a client, where two peer servers co-operate for authentication and if single server is compromised, even in that case also attacker still cannot make believe to be the client with the information from the compromised server. Because no secret word information will be stored and keeps providing services instead of any crash report.

Our two server password authenticated key exchange(PAKE) protocol is symmetric, and runs in parallel in authenticating a client by encrypted key exchange(EKE),providing efficient services to the users. Our protocol applies for the parallel and distributed system where multiple server exist. Performance analysis determines that this protocol is more efficient than existing asymmetric and symmetric two- server PAKE in terms of parallel computing. Security analysis found out to be secure against active and passive attacks, if one server is compromised.

2. RELATED WORK

Earlier secret word-based authentication system transmitted a cryptographic hash value of

the secret word through a public channel; in this case the hash value will be accessible to an unauthorized person. When this is done, it is very frequent for the attacker to work offline, quickly checking out possible secret word against the true password's hash value. Studies have constantly established that a large fractions of user selected secret word are very easily guessable by others. Typical protocols for secret word-based authentication use to stores all the secret words into a single server which is necessary to authenticate clients. If the server is compromise, for example in means of hacking or installation of "Trojan Horse", or it can also even insider attack, the users secret word stored in those server all will be disclosed.

In the existing system were using asymmetric in the sense that one server authenticates the client with help of other server. An asymmetric two-server PAKE runs in series process and only the front-end server and client need to establish a secret session key pattern. Current asymmetric needs to exchange messages for several times in series procedure between two servers. So in turn these are unsuccessful and less efficient than symmetric in which computation is done in parallel order.

3. PROPOSED WORK

In this paper, proposing a new symmetric two server PAKE protocol which supports two servers to work out in similar methodology and works efficiently for practical usage. The protocol requires communication rounds of four for the client and two peer servers mutually to authenticate and simultaneously for establishing secret session keys. In our protocol, we provide one server S1 with an encryption of the secret word E(g2^pw , pk2), and another server S2 with an encryption of the secret word E(g2^pw , pk1), where pk1 and pk2 are the encryption keys of Server1 and Server2, respectively. In addition, two servers are provided random password shares b1 and b2 subject to b1 Ex-or b2 = H(pw), where H is a hash function. The password pw is secret unless the two servers collude, it will not be revealed.

Earlier authentication, each client *C* chooses a password pwC and generates the secret authentication information Auth(1) and Auth(2) for Server1 and Server2, respectively, such that nobody can determine the password pwC from Auth(1) or Auth(2) unless S 1 and S 2 collude. The client sends Auth(1) and Auth(2) to Server1 and Server2, respectively, over different secure channels during the phase of the client registration. Later on, the client remembers only the secret, and the two peer servers retain their password authentication information. According to all existing solutions for two-server PAKE, we assume that never both the peer servers will collude in order to reveal the secret word of the client.

An challenger in our system is either passive or active. We consider both online dictionary attacks, in which any attacker will attempt to login successively, trying every possible secret word, and another offline dictionary attack, in which an adversary drains information regarding the password from observed log sessions. The online dictionary attack is the one which cannot be prevented by cryptographic means but can be easily detected and balanced once the authentication fails several times. The Architecture of symmetric peer server PAKE is exposed in the fig1.

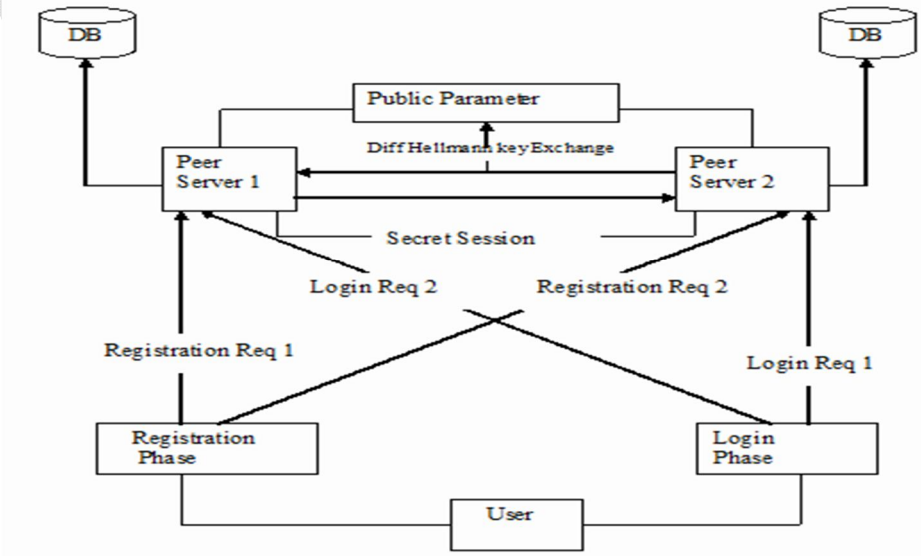

Figure 1 Architecture

Secret Key Establishment:

The J2EE Environment is setup and Two Peer Servers are initialized and release the public parameters for the user by exchange of keys using Diffe-Helman key Exchange. The Secret key is established between Two Servers for further secure communication for Peer Servers. The Secret Session key will ensure that the two servers are Genuinely involved in the process of User Registration and Authentication to provide Peer Services for the Genuine User. Our protocol runs in three phases - initialization, registration and authentication. Of Which Initialization comes Under Secret Key Establishment which uses Diffie-Hellman key Exchange.

System Initialization:

The two peer servers S1 and S2 jointly choose a cyclic group G of large prime order q with a generator g1 .Next, S1 randomly chooses an integer s1 from Z* q and S2 randomly chooses an integer s2 from Z * q , and S1 and S2 exchange g1^s1 and g1^s2 . After that, S1 and S2 jointly publish public system parameters G, q, g1, g2 , where g2 = g^s1s2 .

User Registration and Authentication:

The public parameters released by Peer Servers will be used by client Registration Process, while a user registering to the Peer Services for Encryption of Password Shares and providing Authentication Information to Server 1 and Server 2 Respectively. Registration and Authenticated Key Exchange are the Next Two Phases of our Protocol.

Registration:

We refer to the model of public key cryptosystem, the encryption key of one server should be unknown to another server and the client needs to remember a secret word only after registration. Prior to authentication, each client C is required to register both S1 and S2 through different secure channels. First of all, the client C generates decryption and encryption key pairs (xi, yi) where yi = g1^xi 1 for the server Si (i = 1, 2) using the public parameters published by the two servers.

Next, the client C chooses a password pwC and encrypts the password using the encryption key y, according to El-Gamal encryption.

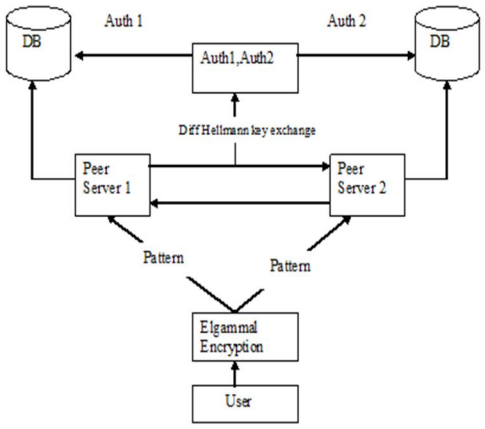

Figure **2 Registration**

At last, the client C delivers the password authentication information Auth(1) C = {x1, a1, b1, E(g2^pwC , y2)} to S1 through a secure channel, and the password authentication information Auth(2) C = {x2, a2, b2, E(g2^pwC , y1)} to S2 through another secure channel. After that, the client C remembers the password pwC only.

Authentication and Key Exchange:

The two servers S1 and S2 have received the password authentication information of a client during the registration. The following steps are involved in the process of Authentication.

1.The client C randomly chooses an integer r from Z * q , computes R = g1 ^ r * g 2 ^ −pwC and then broadcasts a request message M1 = {C,Req,R} to the two servers S1 and S2.

2. The Diffe-Helman Key Exchange Occurs between Peer Servers Which run in parallel and establishes a secret session to fetch the password authentication Information and the two servers mutually generate two values and send Hash functions to Client based on their Password Authentication Informations.

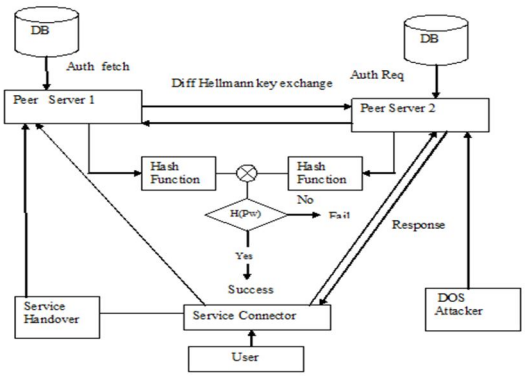

Figure 3 Login

3. The client computes the Hash functions sent and Ex-or ing the Hashes will produce the Hash of his own Password. If the Password Hash and computed Hash are same the client can ensure that he is connected with Genuine Servers and can continue enjoying Services from Peer Servers with out worry.
4. So the user needs to remember the Password Only. Not anything else. He is safe and secure under our Proposed Model.

4. RESULT ANALYSIS

In our system two servers S1 and S2 and a group of the clients. These two peer server cooperate to authenticate clients and services will be provided to the authenticate clients. Our protocols runs through system initialization, secret key establishment, user registration, authentication for peer servers which would give resistance even in case of any distributed denial-of - services.

In the initialization stage S1 and S2 peer servers chooses jointly a cyclic group G of large prime order q with generator g1 and then to exchange, after which release the public parameters. Secret key establishing is use to provide secure communication with peer servers using Diffie Hellman key exchange. Released public parameters by servers will be used by client for registration process, while during this encryption of password shares and authentication information is provided correspondingly. The client computes the hash functions sent and ex-oring the hashes will produce hash of his own password. If the password hash and computed hash are same then client can ensure that connected to the genuine servers and enjoy the services with out worry.

Participants	KMTG Protocol	Our Protocol
Client	comm. $> 15L$ comp. > 20 rounds 3	comm. $3L + 4\ell$ comp. 4 rounds 3
Server	comm. $> 19L$ comp. > 26 rounds 5	comm. $6L + 3\ell$ comp. 5 rounds 4

Figure 4 Performance Comparison of Our Protocol with KMTG Protocol

5. CONCLUSION

In this paper, two peer servers the usage of symmetric protocol for password only authenticated key exchange trustworthiness is given. During authentication phase in case attack, the client can enjoy the service even a server is disclosed by any kind of attacks even if it shuts down manually for new deployment purpose. Session handover mechanisms will handover all
Session during time of attack to other server. So user session will retain safe and will redirect to another server.

REFERENCES

[1].Xun Yi,San Ling,and Huaxiong wang,"Efficient Two-Server Password only Authenticated Key Exchange", IEEE transaction on parallel and distributed system,vol 24,2013.
[2]. 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.
[3]. 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.
[4]. Y. Yang, R.H. Deng, and F. Bao, "A Practical Password-Based Two-Server Authentication and key Exchange System," IEEE Transaction on Dependable and Secure Computing, vol. 3, no. 2, pp. 105-114,Apr.-June 2006.
[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 Int'l Information Security Conf. (SEC'05),pp.95-111,2005.
[6]. 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.
[7]. P. Mackenize, T. Shrimpton, and M. Jakobsson, "Threshold Password-Authenticated key Exchange," Proc. 22nd Ann. Int'l Cryptology Conf. (Crypto '02), pp.385-400,2002.