IMPROVING SERVICE CREDIBILITY IN PASSWORD AUTHENTICATED PEER SERVICES

Nisha.R

PG Scholar, Dept of CSE.

Sri Sairam Engineering College, Chennai-44.

nish.raj25@gmail.com

Uma.R M.E.,(Ph.d)

Professor, Dept of CSE.

Sri Sairam Engineering College, Chennai-44.

uma.cse@sairam.edu.in

Abstract— Two server password-based authentication protocols(Two-Server PAKE), where two servers co-operate to authenticate a client on the basis of password only and if one server is compromised due to insider attack or denial of service attack (DDOS), the attacker still cannot pretend to be the client with the information from the compromised server. Recent research advances in password-based authentication and follow two models. The first model, called Public key infrastructure suggests, that the client having the server's public key in additional to share a password to the server. In this setup, the client has to send the password only to the server by public key encryption (PKE). The second model is called password-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 password-only authentication protocol which is both practical and provably secure under standard cryptographic assumption. Our protocol is symmetric and, can run in parallel to establishes secret session keys between the client and peer servers, respectively. In case any one of the two peer servers shuts down due to the denial-of service attack (DDOS), other server can proceed to provide services to authenticated clients. In case of parallel computation and reliable service, a symmetrical protocol is superior to an asymmetrical protocol.

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

I.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 .Password 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 password authenticated services, to authenticate a client, where two peer

servers co-operate for authentication and if one server is compromised, even in that case also attacker still cannot pretend to be the client with the information from the compromised server. Because no password 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.

II.RELATED WORK

Earlier password-based authentication system transmitted a cryptographic hash value of the password 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, rapidly checking out possible password against the true password's hash value. Studies have consistently proven that a large fractions of user selected passwords are very easily guessable by others. Typical protocols for password-based authentication use to stores all the passwords into a single server which is necessary to authenticate clients. If the server is compromised, for example in means of hacking or installation of "Trojan Horse", or it can also even insider attack, the users password 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 ineffective and less efficient than symmetric in which computation is done in parallel order.

III.PROPOSED WORK

In this paper, proposing a new symmetric two server PAKE protocol which supports two servers to compute in parallel 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 password E(g2^pw , pk2), and another server S2 with an encryption of the password 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.

Prior to authentication, each client *C* chooses a password pwC and generates the password 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 password, 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 password of the client.

An adversary 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 password, 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 suspended once the authentication fails several times. The Architecture of symmetric peer server PAKE is shown in the figure1

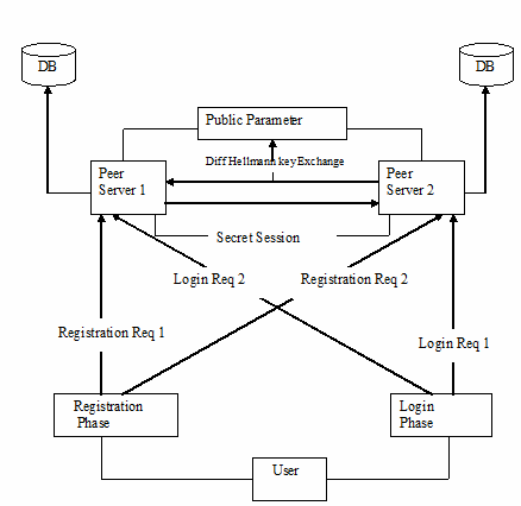

Fig 1 Architecture

IV.IMPLEMENTATION

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.

Fig 2 Implementation

V.CONCLUSION

In this paper, two peer servers the usage of symmetric protocol for password only authenticated key exchange credibility 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.

VI.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 Trans. 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.