ISSN:2231-0711

Nishikant S. Burande et al | IJCSET(www.ijcset.net) | November 2015 | Vol 5, Issue 11,383-384

Design Model for Two Server Password Authentication Protocol

Nishikant S. Burande[#1], Prof. Kahate S.A.[*2]

[#1 , *2]*Dept. of Computer Engineering, SPCOE, Otur SavitribaiPhule Pune University, India*

Abstract— **In this paper a two server password authentication protocol described. In the sense that two symmetric servers are used for the authentication purpose with making preliminary caution that if one server shut down due to some reason then another server should continue to provide the services to the client. Many protocols are established for the security in server. Client communicates to server through two different secure channels. The authentication information of client on server1 is kept with backup on server2 and vice versa. For avoiding the data redundancy the periodic backup facility is adopted in this system. In this way two server authentications with backup can be created.**

Keywords— **PAKE, Diffie-Hellman, Elgamal Encryption**

I. INTRODUCTION

Many users choose a low entropy password. So that hacker can easily get that passwords and misuse the account details of the user. Also if server is compromised then also user passwords are disclosed to the user. To avoid such difficulties, two server password based authentication scheme has been established. Traditional protocols for password based authentication system used single server. Here it is considered two servers. Single point of failure issue are arises when single server attacked by attacker. Server may disclose all the passwords to the attacker in offline dictionary attack also. Here considered scenario if one of the servers shut down due to some reason then another server should continue to provide services to the clients. This is very necessary to take backup periodically because backup may result in the data redundancy.

II. LITURATURE SURVEY

In recent years, to prevent from Offline dictionary attack and to prevent from attacker from misuse of the password many authentication systems are established and proposed. To solve such type of problem, another kind of authentication system called the multiple server authentications was proposed. In that manner, the capability to verify a password is split between two or more servers, this secures system from intruders. In such multiple server authentication system, Two server authentication system more simple acceptable by the users. Many two server system discussed and reported

Next Yang proposed a new technique [1], for the prominent functionality.previously also some of them are mentioned as follows.Two server password system in which one server(called Blue server or service server, SS for short) exposes itself to users and the other(called Red server of Control server, CS for short) is hidden from clients is proposed by Brainard et al's[2]. This is not password only system. It is very interesting two server system.A robust finger print based two-server authentication system and key exchange system proposed by Mukesh et al's[3]. This was the first two server finger print based authencation system. In that system user passwords are replaced by fingerprint template of the user of the system User didn't need to remember it. Both the servers' should have to public keys to protect the communication channel from users to servers. XunXi[5] also provide security threats for the two server authentication technique. Then the Jiang Huiping[6] also provided the strong password authentication scheme for the two server password protocol. In recently, practical approach proposed by Yang et al.[1] and an efficient password-only two-server authenticated key exchange system, this scheme is a password only variant of the one introduced by Brainard et al.'s None of the existing two-server password based authentication schemes enables a user to use the same password over multiple service servers, which is deemed an important feature of the two-server model. Then ShuoZhai. [7] proposed a two server password only authenticated key exchange the authors mentioned that this is the first provably secure two-server protocol for the important password-only setting(in which the user need remember only a password, and not the servers public keys), and this was the first two server protocol(in any setting) with a proof of security in the standard model.

III.TWO SERVERS WITH PERIODIC BACKUP

Here it is described that the how system going to work, in another way this paper describes the design model for the two server password authentication protocol. Here client needs to register on both the servers. After registering on both the server both have auth1 and auth2 information of the client on server S1 and server S2 respectively. Server S1 and Server S2 communicate to each other for the authentication of the client. Client should know the password also the public of the server. System have the periodic backup facility, here assumption isthat new clients can be able toregister on system if both server are working. If one of the two server is not working then only old client only login to the system. some of the screen shot of the system are as follows:

Fig.3.1 Registration Phase

Fig. 3.2 Authentication Phase

IV. EQUATIONS

4.1Elgamal Encryption

Each user has a private key x
Each user has three public keys: prime modulus p, generator g and public Y = gx mod p
Security is based on the difficulty of DLP
Secure key size > 1024 bits (today even 2048 bits)
Elgamal is quite slow, it is used mainly for key authentication protocols

V. ALGORITHMS

Diffie–Hellman key exchange is ageneral method to exchange cryptographic keys. This is one of the most popular practical examples of key exchange that is implemented in the field of cryptography. The Diffie–Hellman key exchange method allows client and server that have no any knowledge about each other to jointly establish a shared secret key over an insecure communicationschannel. This key can then be used to encrypt subsequent communications using a symmetric keycipher. In cryptography technique, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. This was described by Taher Elgamal in 1984. ElGamal encryption method is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. Digital signature algorithm is also a variant of the ElGamal signature scheme, which is different than Elgamal Encryption scheme.

VI. BACKUP TECHNIQUE

In this paper it is considered that periodic backup technique has been used. This technique is used because of the reason to avoid the data redundancy. As My-Sql Data base is a suitable for these types of techniques. There are many techniques of backup are also there like incremental backup technique and so on.
Following is the basic syntax to take backup in My-SQL:

15 2 * * * root mysqldump -u root -pPASSWORD --all-databases | gzip> /mnt/disk2/database_`data ' %m-%d-%Y'`.sql.gz

If one of the server shut down due to some reason then another server can continue to provide services to the registered client this is the main aim of this provide. Here backup of server S1 is stored on Server S2 and vice versa. In this way backup technique is used. Backup is taken automatically from server S1 and Server S2.
And the case when one of the server shutdown due to some reason. Then that backup is used for the another server to restore the data at the current state. And the system should regain its working. In this way it can be found very suitable and secure system for the security purposes.

VII. CONCLUSION

In this paper firstly it described about the two server authentication schemes. Then public key, authentication information is also described. This protocol provide secure against active and passive attack also. Elgamal encryption and Diffie-Hellman algorithms are basic of the encryption and decryption technique.

REFERENCES

[1] Yanjiang Yang, “Enabling Use of Single Password over Multiple Servers in Two-Server Model ”, Computer and Information Technology (CIT), 2010 IEEE 10th International Conference.
[2] B. Kaliski and M. Szydlo J. Brainard, A. Juels.Nightingale: “A new two-server approach for authentication with short secrets”, in Proceedings of the 12th USENIX Workshop on Security, pages 1-2. IEEE Computer Society, 2003.
[3] Mukesh, R.Damodaram, A.SubbiahBharathi,V. “A robust fingerprint based twoserverauthentication and key exchangesystem”, 3rd International Conference on Communication Systems Software and Middleware and workshops, 2008 Bangalore, pp. 167-174.
[4] DexinYang , Bo Yang “A Novel Two-Server Password Authentication Scheme with Provable Security”, IEEE Transaction 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).
[5] Xun Yi, “Security Analysis of Yang et al.'s Practical Password-Based Two-Server Authentication and Key Exchange System”, 2011 4th International Conference. Network and System Security (NSS).
[6] Jiang Huiping. “Strong password authentication protocols”, 2010 4thInternational Conference Distance Learning and Education (ICDLE).
[7] ShuoZhai, “Design and implementation of password-based identity authentication system”, 2010 International Conference Computer Application and System Modeling (ICCASM).