ISSN : 2231-0711

Nishikant S. Burande et al | IJCSET(www.ijcset.net) | July 2015 | Vol 5, Issue 7,229-231

Symmetric Two Server Password Only Authenticated Key Exchange with Periodic Backup

Mr. Nishikant S. Burande[#1], Dr. S.V. Gumaste[*2]

[#]*Computer Engineering, SPCOE, Otur*
SPPU, Pune, India.

[*]*Associate Professor, Computer Engineering, SPCOE, Otur*
SPPU, Pune, India

***Abstract*— Two Server Password only authenticated key exchange protocol is most secure technique. It avoids dictionary attack and other threats. By using two servers it is possibility that one of server may shut down due to some reason. So system will collapse. To continue with the system with this fault, making extension of taking periodic backup facility. Because if only backup is taken then there is possibility of redundancy. Here backup are stored on both Server1 and Server2, Server1 will store backup of Server2 and vice versa.**

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

I. INTRODUCTION

Two Server authentication techniques is very secure technique for storing and authenticating system. Symmetric two server system is reliable than Asymmetric system. As recent advance research 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.

Basically there are two models PKI based and Password only model. In most of the cryptographic technique Diffie-Hellman Key exchange protocol and Elgamal Encryption algorithm are used. Both these algorithms provide a base for encryption and decryption purpose. When using two server, it avoids the disadvantages of Trojan horse, dictionary attack etc.

Here proposed a protocol as pw=pw1+pw2. Pw1 and Pw2 both contain authentication information as auth1 and auth2. This protocol follows Password only model of authentication purpose.

Security analysis has shown that this protocol is secure against active and passive attack. In 2013 Xun Yi, San Ling, and Hoaxing Wang [1] shown the security analysis about efficient two server password only authenticated key exchange. That protocol provided more security for authentication purpose.

Based on the identity-based encryption technique Yi et al. suggested an identity-based model where the client needs to remember the password only while the server keeps the password in addition to private keys related to its identity. In this setting, the client can encrypt the password based on the identity of the server. This model is between the PKI-based and the password only models.

This protocol can be applied in distributed systems where multiple servers exist. For example, microsoft active directory domain service (AD DS) 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 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, So can split the user's 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, achieve more secure AD DS.

Here provided the periodic backup facility to avoid the if one of server may shut down due to some reason. If that happen then another server can continue to work. When one server continued to work only registered clients can use the system, till new registrations are not allowed.

II. LITERATURE SURVEY

In case of single server password only authenticated key exchange protocol, if the server is compromised, user passwords stored in the server are all disclosed. To overcome this issue ford and kaliski[2]. In 2003 Brained et al. [3] developed the first two server protocol in the PKI based setting.

Later on a similar type of research has been done by the Stevan M. Bellovin and Micheal Merrit[4] their main goal was to protect the peoples with weak passwords. Empirically, weak passwords are fact of life attempt to strengthen users passwords by enforcing syntactic rectrictions was not successful. They have proposed EKE protocol, that can be used from dictionary attack. EKE can be used with verity of asymmetric cryptosystem and public key distribution system. They also used basic protocol as Diffie-Hellman Key Exchange protocol[5] using EKE is quite similar to using it with any conventional asymmetric cryptosystem.

To solve the issue of dictionaray attak Xun yi, Raylin Tso, and okamoto[6] had proposed Group password based authentication. In case of this technique a group of clients have been considered with one server and eah of clients shares a secret key(group key) with the help of the server. Here each client needs to remember only password while server keeps the private key. They proposed a KE compiler for the group keys. The basic idea of this compiler is that users of a group firstly run the group KE protocol to establish a group key without any help of the server, and then the server helps users of the group with utual authenticatin and key onfirmation by the shared password(prototected with the IBE scheme), and finally eah user authenticated the server, along with partnered users and the established key during the group. This model assumes that all users and servers refer to the common public parameters including the public key of a private key generator(commonly used in ID-based model). Also this model is ID-Based, where the public key of a server is its identity(which is meaningful) and public key authentication is unnecessary. Thus, the public key infrastructure(PKI) is not needed in their model. Similar to the Katz-Ostrovsky-Yung[7] model.

Next Jonathan Katz, Philip Mackenziey, Gelareh Tabanz, Virgil Gligorx[8] had worked on two server authentication protocol. They worked two server version of password only authentication key exchange protocol Katz, Ostrovsky, and Yung(the KOY protocol). This was the first secure two server protocol. As this is the most efficient two server authentication protocol. They assume that every client C in the system shares its password pw with exactly two servers A and B. In this case servers A and B are associated with Server C.(A Single server may be associated with multiple clients.). In addition to holding password shares, these servers may also be provisioned with arbitrary other information(that need not be stored by C). Any such information is provisioned by some incorruptible, central mechanism(a system administrator, say) at the outset of the protocol. This does not represenet a restriction in practice, since the servers must be provisioned with correct password shares anyway, and so any additional information can be provided to the servers at that time.

Also to solve the issue of easily guessed password, threshold based password technique in PKI based model used by the Ford and kaliski[9] in which n servers are co-operate to each other for authentication. This is secure till n-1 servers are being compromised. In the next joblon[10] removed the requirement of PKI based and used the public key encryption. Next, in 2005, Katz et al.[5] proposed the first two server password only authenticated key exchange protocol with a proof of security in the standard model. The advantage of this protocol is the structure which supports two servers to compute in parallel and disadvantage is inefficiency for practical use. Yang et al.[7] suggested an Asymmetric setting, where 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 secret session key in the end.

III. PRELIMINARIES

A. *Diffie-Hellman Key Exchange Protocol*

Diffie-Hellman establishes a shared secret that can be used as secret communications for exchanging data over a public network. To implement Diffie-Hellman [11], the 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 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 hole number m and n, Next, Alice and Bob compute public keys A

and B based on their personal keys according to the formulas.

$$A = g^m \bmod p$$
$$B = g^n \bmod q$$

B. *Elgamal Encryption scheme*

Security points about elgamal encryption key exchange protocol are:

- Each user has three public keys: prime modulus p, generator g and public Y=gx mod P
- Secure key size more than 2048 bits
- Elgamal Authentication is slow it is mainly used for

key authentication protocol Now widly used.

IV. PROPOSED SYSTEM

This paper describe about the implementing a two server authentication system, in which basically authentication is done by using the Diffie-Hellman algorithm. Also overcoming the disadvantage of existing system that if one server shut down due to some reason so that also our proposed system will work fine. For the purpose keeping backup file of Server S1 on Server S2 and vice-versa. By using backup files system will work for 48hrs. so need to recover the damaged server within 48hrs.

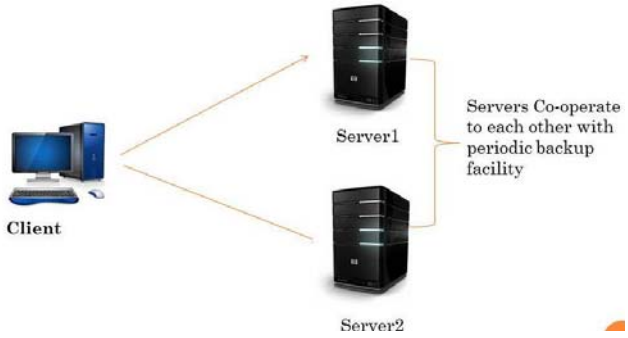

Fig1: system architecture

Fig1 shows about the system architecture, here two servers are there, client is authenticated by two servers only. It avoids dictionary attacks. As both the servers contribute equally to the system so these servers are symmetric servers.

V. CONCLUSIONS

Here proposed the various PAKE protocol. Two types of servers are also explained that are symmetric and asymmetric . Diffie-Hellman and Elagamal encryption algorithms are basic building blocks of the explained protocol. Here it is important to consider that if one server shutdown due to some reason then there is facility to the servers to take periodic backup. By using periodic backup technique the redundancy in the data an be avoided. Security propose that it is ery important and efficient protocol. Mainly this protocol uses the public key encryption so that communication is done through secure channel instead of broadcasting from client to the servers. After security analysis it is come to know that this protocol secure against active and passive attack.

REFERENCES

[1] Xun Yi, San Ling, and Huaxiong Wang, " Efficient Two Server Password-Only Authenticated Key Exchange" IEEE Transactions on Parallel and Distributed System Vol-24 No: 9 Year 2013

[2] W. Ford and B.S. Kaliski Jr., "Server-Assisted Generation of a Strong Secret from a Password," Proc. IEEE Ninth Int'l Workshop Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 176-180, 2000.

[3] 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.

[4] S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocol Secure against Dictionary Attack," Proc. IEEESymp. Research in Security and Privacy, pp. 72-84, 1992.

[5] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, IT-22, no. 6, pp. 644-654, Nov. 1976.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] D. Jablon, "Password Authentication Using Multiple Servers," Proc. Conf. Topics in Cryptology: The Cryptographer's Track at RSA (RSA-CT '01), pp. 344-360, 2001.