Two Servers Password Authentication with Results

NishikantS. Burande[1] Prof. Kahate S.A.[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]SPCOE, Otur SavitribaiPhule Pune University, India

Abstract— There are many ways to use two servers for authentication purpose like symmetric and asymmetric authentication servers. In symmetric authentication server two servers contribute equally to each other for the authentication purpose. In asymmetric two servers one server helps to another server for the authentication purpose. In this paper two symmetric servers for the purpose of authentication. This is first system that providing periodic backup facility. Also it is showed here that how the two server contribute equally in process of password authentication scheme. Client can share files from another client or to the another client. This phenomenon provides security against active attack and passive attack also.

Key words: Private Key, Periodic Backup, Elgamal Encryption, PAKE

I. INTRODUCTION

Password are used for security purposes to secure email account, bank account, users data and so on for that cryptographic techniques are being used. In the same manner a system user may require password to access their email account, bank account, computer password and many more. Earlier password based authentication system are protected by using cryptographic key that key can be sent over a network worth public channel, that hash value can be easily accessible to the attacker. This technique is not secure as attacker can do the offline attack on the system and they can hack all the passwords stored on the system. Studies consistentantly shown that many password can be easily guessed by the attacker. Many studies have shown tha t about cracking/guessing the users passwords within very less time.so it is necessary to have a authentication information along with the password so that user account are secure. Currently there are two authentication models are there. In the first model clinet keep the authentication information of server along with password this model is called PKI based model. In this technique client can send public key to server by public key encryption. Gong et al was the first to provide this kind of security. Second model is password only model. Bellovin and Merrit are first to introduce this kind of model. Formal models of security for the password-only authentication were first given independently by Bellare et al. and Boyko et al. Katz et al. were the first to give a password-only authentication protocol which is both practical and provably secure under standard cryptographic assumption. 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.

Here user will register to server1 and then to server2. The encryption key received from server 1 need to authenticate towards server2. File sharing also possible with the help of this kind of encryption key.

II. LITERATURE SURVEY

Firstly Abdala[1] provided the simple password based authentication model using two server. Then next M. Abdalla, O. Chevassut, and D. Pointcheval are provided solution for the purpose of one time verifier scheme for the authentication purpose. M. Bellare, D. Pointcheval, and P. Rogawa[3] provided solution against to secure from the offline dictionary attack. In the next S. Bellovin and M. Merritt also provided the enhanced security against the dictionary attack[4]. S. Bellovin and M. Merritt[5][6] provide very secure technique for the purpose authentication purpose against the threats. V. Boyko, P. Mackenzie, and S. Patel[7][8] also provided the protocol security purposes against the dictionary attack and so. J. Brainard, A. Jueles, B.S. Kaliski, and M. Szydlo[9] provided a new way for authentication purpose with shortsecret. M. Di Raimondo and R. Gennaro[10] provided threshold based security technique. O. Goldreich and Y. Lindell[11] provided with session key generation security technique. D. Jablon[12] provided a way of security with multiple server authentication.] H. Jin, D.S. Wong, and Y. Xu[13] provided a way of efficient two server authentication key exchange system. These are many techniques that are proposed by previous authors. But they not have been mentioned about the suppose one server fails then how another server going to provide services to the clients. Here it is made that periodic backup facility as server1 backup will be stored on server2 and vice versa. Suppose one of the servers fails then also system will continue to provide the services to the clients. Here it is taken periodic backup to overcome the issue of the data redundancy.

III. IMPLEMENTATION DETAILS

A. Registration

The two secure channels are necessary for all twoserver PAKE protocols, where a password is split into two parts, which are securely distributed to the two servers, respectively, during registration. Although we refer to the concept of public key cryptosystem, the encryption key of one server should be unknown to another server and the client needs to remember a password only after registration.

B. Authentication

Next is the authentication phase, in this phase authentication has been done. Two Auth1 and Auth2 information is required for the authentication purpose.

C. Module Description

1) Diffie-Hellman Key Exchange Protocol

The Diffie-Hellman key exchange protocol was invented by Diffie and Hellman in 1976. It was the first practical method for two users to establish a shared secret key over an unprotected communications channel. Although it is a non-

authenticated key exchange protocol, it provides the basis for a variety of authenticated protocols. Diffie-Hellman key exchange protocol was followed shortly afterward by RSA, the first practical public key cryptosystem.

2) ElGamal Encryption Scheme

Each user has a private key x

Each user has three public keys: prime modulus p, generator g and public Y = gxmod 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

3) Initialization

The two peer servers S1 and S2 jointly choose a cyclic group G of large prime order q with a generator g1 and a secure hash function H: {0; 1}*->Zq, which maps a message of arbitrary length into an l-bit integer, where l= log2 q. Next, S1 randomly chooses an integer s1 from Zq and S2 randomly chooses an integer s2 from Zq , and S1 and S2 exchange g1s1 and g1s2. After that, S1 and S2 jointly publish public system parameters G; q; g1; g2;H where g2 = gs1s2.

IV. SHARING FILE CLIENT TO CLIENT

For sharing a file from one client to another client it need the know the private key in addition to the password. Private key is can be found by the use of Diffie-Hellman Key exchange and Elgamal encryption scheme.

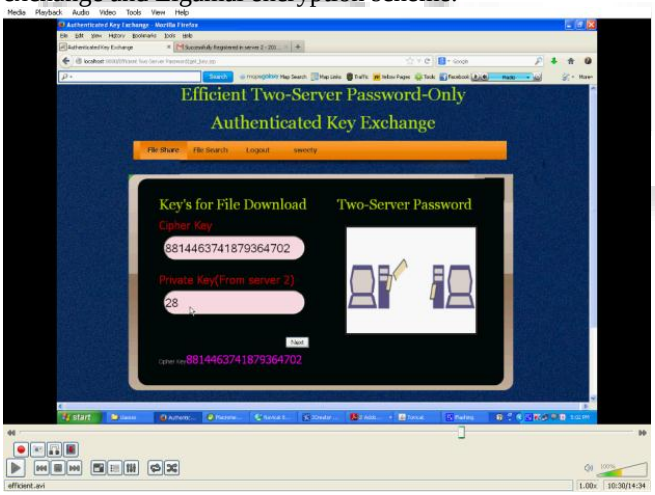

Fig. 1: sharing a file from one client to another client

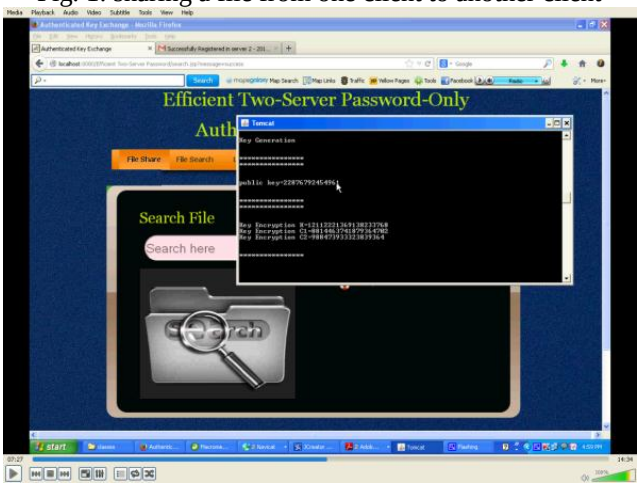

Fig. 2: sharing a file from one client to another client

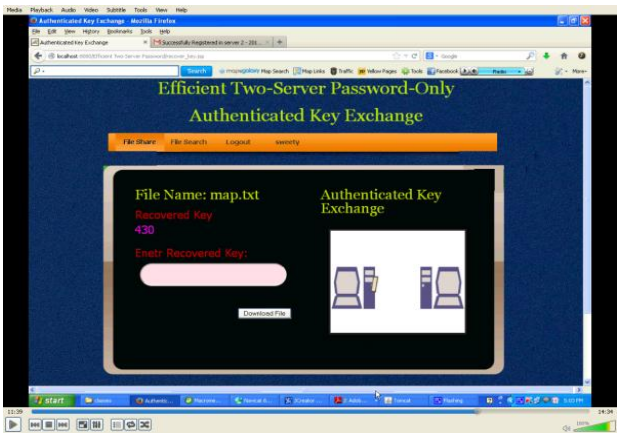

Fig. 3: sharing a file from one client to another client

V. RESULTS AND DISCUSSIONS

Here it is considered by registering different users with the system. First user need to register to Server1 and then Server2. Private Key is sent by mail to the user. User need to use that private key while the sharing the file to another client or to find the shared file by another user. here it can be found this protocol provides major solution to the dictionary attack. Near about 20 passwords are stored in system for experimental results and found that that are uncrackable by attacker, when attacker attack on system he cannot get the information about the password. Because to reveal the password it is necessary to two server should contribute. Elgamal encryption and Diffie-Hellman algorithm plays important role here.

Further details are shown this protocol is most secure as stated earlier protocols. Prime number consideration is very important thing in this phenomenon. Prime numbers are choosen randomly in this technique.

VI. FUTURE ENHANCEMENT

In terms of parallel computation, our symmetric protocol has a feature that the total running time for t two server side is equal to the total running time of one server, i.e., transmitting 6L þ 3‘ bits and computing five modular exponentiations in four rounds. However, in the asymmetric YDB protocol and the asymmetric JWX protocol, the total running time in the two-server side is equal to the sum of two servers’ running time, i.e., transmitting 8L þ 3‘ bits and computing nine modular exponentiations in 10 rounds in the YDB protocol, and transmitting 11L þ 3‘ bits and computing 12 modular exponentiations in six rounds in the JWX protocol. Even if the precomputation is allowed, the two servers in the YDB protocol or the JWX protocol still need to compute seven modular exponentiations in series. Therefore, this protocol is more efficient than the asymmetric YDB protocol and the asymmetric JWX protocol in terms of the total running time.

This protocol needs more storage for keeping the password authentication information in the two servers than the YDB protocol and the JWX protocol.

VII. CONCLUSION

Here it is observe red that instead of using one server for the authentication purpose; need to use two servers for the authentication purpose. As suppose one of the server is

compromised then another server can continue to provide the services to the clients. After the recovery time both the servers can work fine. As both the server stores each other's periodic backup. So as to it avoids the data loss occurs during the failure of the server. This presents that protocol is secure against dictionary attack also.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[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] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. (Crypto '01), pp. 213-229, 2001.
[6] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586- 615, 2003.
[7] D. Boneh, "The Decisional Diffie-Hellman Problem," Proc. Third Int'l Algorithmic Number Theory Symp., pp. 241-250, 1998.
[8] 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.
[9] 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.
[10] M. Di Raimondo and R. Gennaro, "Provably Secure Threshold Password Authenticated Key Exchange," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt '03), pp. 507-523, 2003.
[11] 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.
[12] 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.
[13] H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password Only Two- Server Authenticated Key Exchange System," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.

