International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey on Public key Encryption for Two Server Password only Authenticated Key Exchange

Nishikant Burande[1], Gumaste S.V.[2]

[1]Sharadchandra Pawar College of Engineering, (Pune University), Dumbarwadi, Otur, Pune

[2]Professor & Head, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune

Abstract: ***By using cryptographic key client and server establishes a connection in between them and authenticate each other. In other words they use password to authenticate that is Password-authenticated key exchange (PAKE). The password necessary to authenticate are stored in a single server. If server is hacked or due to insider attack it is compromised then all password may stole by hacker and they may misuse it. In this paper find a way to overcome this problem by using two servers to authenticate in which two servers cooperate to each other. If one server is compromised then attacker still cannot hack the passwords stored in server. For the said purpose two ways are there symmetric & asymmetric, in symmetric two servers equally contribute and in asymmetric one server authenticates the client with the help of another server. This paper presents a symmetric solution for two-server PAKE, where client can establish different cryptographic keys with two servers' resp. Proposed protocol runs in parallel and is more efficient than existing symmetric two-server PAKE protocol.***

Keywords: Cryptography, password only authenticated exchange, Diffie-Hellman key exchange, ElGamal encryption

1. Introduction

For the login process the passwords are commonly used by people. To control access to email accounts, Operating systems, mobiles, T.V., Automated Teller Machine etc. they require password. A computer user requires a password for many purposes like accessing websites. In another way people keep security to system by using passwords. Earlier security solutions provide the solution as public key cryptographic hash values on public channel. On which attacker can easily find the hash value and attack on the system. This is very common and attacker can work offline also. Studies have shown that many passwords guessed by the attacker so it is easy to them to hack the accounts. For example, according to Bruce Schneier, examining data from a 2006phishing attack, 55 percent of MySpace passwords would be crackable in 8 hours using a commercially available Password Recovery Toolkit capable of testing 200,000passwords per second in 2006[1]. Current research studies show that client and server first have to authenticate each other via secure communication channel and they can make conversations. Currently password based authentication follows two models. The first model, called PKI(public key interface)-based model, assumes thatthe client keeps the server's public key in addition to share a password with the server. Gong et al. [2], [3] where the first to show this kind of authentication protocol. Formal Definitions are firstly provided by Halevi and Krawczyk [13]. The second model is Password only model. This is also called as "encrypted key exchange" protocol, where the password is used as a secret key to encrypt random numbers for key exchange purpose. This kind of model was first proposed by Bellovin and Merritt [4].Based on the identity-based encryption technique [5], [6], Yi et al. [7], [8], [9] 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. Generally all protocols consider that all the passwords are stored on single server and client can remember a particular password associated to it. But there will be problem like if the server is compromised due to insider attack, denial of service attack the user passwords are all disclosed. To overcome this issue two server authentication models are introduced in [10], [16], [20],[21], [22], and [14], Where two server cooperate to each other to authentication purpose. If one server is compromised due to attack still attacker cannot pretend to disclose the passwords. Current solutions for password Authenticated key exchange(PAKE) either symmetric in which two servers contributes equally such as[16] or asymmetric in the sense authentication of one server is done with the help of another server such as[21],[14]. Katz et al.'s two-server PAKE protocol[16] suggest that for symmetric method client establishes a secret session keys between client and two servers. If one server shut down due to some attack still another server can continue to provide service to the clients. Only Katz et al's two server[16] protocol is symmetric and not efficient for practical use.

On the other hand asymmetric protocol runs in series manner. Client sends request in form of cryptographic key for authentication towards front server then with the help of backend server. Yang et al [21],[22] and Jin et al [14] are asymmetric protocol. Symmetric design is more efficient than asymmetric design. Symmetric design provides parallel computation while asymmetric design provide series computation.

This paper proposes a system which is symmetric. When client want authenticate with its accounts which are password protected. The authentication process is done with two servers. Client sends a cryptographic key in parallel manner to two servers S1 and S2 as pw1 and pw2 resp., pw=pw1+pw2 and then authentication done. This protocol follows password-only model. Encryption key pairs and decryption key pairs are generated by clients and sent to Server S1 and Server S2. If one server shut down then also

this system will work as Server S1 have backup files of server S2 and vice versa. But that back up will work only for 48hrs. So need to recover damaged server within 48hrs for establishment of such type of system use Diffie-Hellman key exchange protocol and Elgamal Encryption scheme.

This protocol can be used for multiple servers that are in distributed system for example Microsoft active directory domain (AD DS). 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. . 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 two-server PAKE protocol and 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, this can achieve more secure AD DS.

The remainder of this paper organized as follows, in section 2 provided literature survey. Section 3 contains basic protocols for implementation. Section 4 contains symmetric model for password authentication. Section 5 contains security analysis and last section contains the conclusion.

2. Literature Survey

In case of single-server PAKE protocol, if the server is attacked or compromised, user passwords stored in the server are all disclosed. To address this issue, in 2000, Ford and Kaliski[12] proposed the first threshold PAKE protocol in the PKI based model, in which n servers cooperate to authenticate a client. Their protocol remains secure as long as n-1 or few servers are compromised. Subsequently, in 2001, Joblon[14] removed the requirement for PKI and suggested a protocol with the similar property in the password-only model. Both the threshold PAKE protocols were not shown to be secure formally. In 2002, MacKenzie et al. [17] gave a protocol in the PKI-based setting, which requires only t outof n servers to cooperate to uthenticate a client and is secure as long as t-1 or fewer servers are compromised. They were the first to provide a formal security proof for their threshold PAKE protocol in the random oracle model. In 2003, Di Raimondo and Gennaro [11] proposed a protocol in the password-only setting, which requires less than 1/3 of the servers to be compromised, with a formal security proof in the standard model.

In 2003, Brainard et al. [9] developed the first two-server protocol in the PKI-based setting. Their protocol and its variant [19] assume a secure channel between the client and the server(s), which would be in practice implemented using public key techniques such as SSL. In 2005, Katz et al.[16] proposed the first two-server password-only authenticated key exchange protocol with a proof of security in the standard model. Their protocol extended and built upon theKatz-Ostrovsky-Yung PAKE protocol [15], called KOY protocol for brevity. In their protocol, a client C randomly chooses a password pw, and two servers A and B are provided random password shares pw1 and pw2 subject to pw1 + pw2 = pw. At high level, their protocol can be viewed as two executions of the KOY protocol, one between the client C and the server A, using the server B to assist with the authentication, and one between the client C and the server B, using the server A to assist with the authentication. The assistance of the other server is necessary since the password is split between two servers. In the end of their protocol, each server and the client agree on a secret session key. Katz et al.'s protocol [16] is symmetric where two servers equally contribute to the client authentication and key exchange. For their basic protocol secure against a passive adversary, each party performs roughly twice the amount of works as the KOY protocol. For the protocol secure against active adversaries, the work of the client remains the same but the work of the servers increase by a factor of roughly 2-4. The advantage of Katz et al.'s protocols is the protocol structure which supports two servers to compute in parallel, but its disadvantage is inefficiency for practical use. Built on Brainard et al.'s work [9], in 2005, Yang et al. [20]suggested an asymmetric setting, where a 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 a secret session key in the end. They proposed a PKI-based asymmetric two-server PAKE protocol in [20] in 2005 and several asymmetric password-only two-server PAKE protocols in [21] and [22] in 2006. In their password-only protocol [21], [22], the client initiates a request, and SS responds with B = B1B2, where $B1 = g1^{b1}g_2^{\pi 1}$ and $B2 = g1^{b2}$ $g2^{\pi 2}$are generated by SS and CS on the basis of their randompassword shares π_1 and π_2, respectively, and then the client can obtain $g1^{b1+b2}$ by eliminating the password $\pi(=\pi 1+\pi 2)$from B, i.e., computing B/g_2^{π}.

Next, SS and the client authenticate each other by checking if they can agree on the same secret session key. The security of Yang et al.'s protocol in [21] is based on an assumption that the back-end server cannot be compromised by anactive adversary. This assumption was later removed in [22]at the cost of more computation and communication rounds. The advantage of Yang et al.'s protocols [21], [22]is efficiency for practical use. Yang et al.'s protocols are more efficient than Katz et al.'s protocols [16] in terms of communication and computation complexities, but its disadvantage is the protocol structure which requires two servers to compute in series and needs more communication rounds. In 2007, Jin et al. [14] further improved Yang et al.'s protocol [22] and proposed a two-server PAKE protocol with less communication rounds. The advantage of Jin et al.'s protocol is that itneeds less communication rounds than Yang et al.'s protocol in [22] without introducing additional computation complexity. Like Yang et al.'s protocols, the dis-advantage of Jin et al.'s protocol is the protocol structure which requires two servers to compute in series.

In this paper, proposed a new symmetric two-server PAKE protocol which supports two servers to compute in parallel and meanwhile keeps efficiency for practical use. This protocol needs only four communication rounds for the client and two servers mutually to authenticate and simultaneously to establish secret session keys. This protocolis more

efficient than existing symmetric two-server PAKE protocol, such as Katz et al.'s protocol [16]. In terms of parallel computation, This protocol is even more efficient than existing asymmetric two-server PAKE protocols, such as Yang et al.'s protocol [21] and Jin et al.s protocol [14].

3. Prilimaniries

3.1 Diffie-Hellman Key Exchange

Cryptographers face a major problem in case of Public-key algorithms that is key exchange. The problem of key exchange solved in 1976 by Diffie and Hellman at standforduniversity[10]. That protocol known as Diffie-Hellman key exchange protocol. This protocol followed by RSA[18] algorithm, the first practical method of public key encryption.

The representation of Diffie-Hellman Algorithm illustrated below.

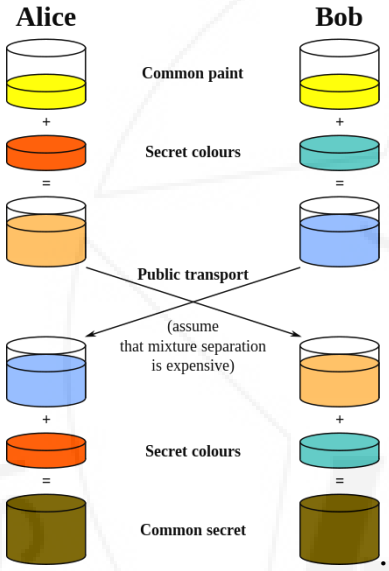

Figure 3.1: Illustration of Diffie Hellman Algorithm

4. 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 and also overcoming the disadvantage of existing system that if one server shut down due to some reason so that also 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.

5. Security Analysis

The security analysis shows that the security features which the proposed protocol should satisfy. It is desirable for a Two-Server PAKE protocol to possess the following security attributes [15]:

a. Forward secrecy: If the user's password or the server's private key is divulged, the secrecy of previously established session keys should not be revealed.
b. Known session key security: Disclosure of one session key should not reveal other session keys.
c. Resilience to Denning-Sacco attack: Disclosure of session key should not enable an attacker to calculate or guess the password.
d. Resilience to password compromise impersonation attack: Password compromise of any user A should not enable an at-tacker to share any session key with A by impersonating him-self/herself as any other entity.
e. Resilience to Unknown Key Share (UKS) attack: User A should not be coerced into sharing a key with an attacker while he thinks that his key is shared with another user B.
f. Resilience to off-line dictionary attack: If an attacker could guess a password, he should not be able to check his guess off-line.
g. Resilience to undetectable on-line dictionary attack.

6. Conclusion

This is the survey of different types of PAKE protocols that are in existence. Basically Diffie-Hellman key exchange protocol is most important among described above. Also considered the scenario that among two server if one server shut down then also how system will continue to work.

References

[1] http://www.schneier.com/blog/archives/2006/12/realworld_ passw.html, 2013.
[2] L. Gong, T.M.A. Lomas, R.M. Needham, and J.H. Saltzer, "Protecting Poorly-Chosen Secret from Guessing Attacks," IEEE J. Selected Areas in Comm., vol. 11, no. 5, pp. 648-656, June 1993.
[3] T.M.A. Lomas, L. Gong, J.H. Saltzer, and R.M. Needham,"Reducing Risks from Poorly-Chosen Keys," ACM OperatingSystems Rev., vol. 23, no. 5, pp. 14-18, 1989.
[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] 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.
[8] 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.
[9] X. Yi, R. Tso, and E. Okamoto, "Identity-Based Password- Authenticated Key Exchange for

Client/Server Model," Proc. Int'l Conf. Security and Cryptography (SECRYPT '12), pp. 45-54, 2012.
[10] 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.
[11] X. Yi, R. Tso, and E. Okamoto, "Identity-Based Password-Authenticated Key Exchange for Client/Server Model," Proc. Int'l Conf. Security and Cryptography (SECRYPT '12), pp. 45-54, 2012.
[12] 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. 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] S. Halevi and H. Krawczyk, "Public-Key Cryptography and Password Protocols," ACM Trans. Information and System Security, vol. 2, no. 3, pp. 230-268, 1999.
[14] 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.
[15] J. Katz, R. Ostrovsky, and M. Yung, "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (Eurocrypt '01), pp. 457-494, 2001.
[16] 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.
[17] 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.[11] M. Di Raimondo and R. Gennaro, "Provably Secure ThresholdPassword Authenticated Key Exchange," Proc. 22nd Int'l Conf.Theory and Applications of Cryptographic Techniques (Eurocrypt '03),pp. 507-523, 2003.
[18] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.
[19] M. Szydlo and B. Kaliski, "Proofs for Two-Server Password Authentication," Proc. Int'l Conf. Topics in Cryptology (RSA-CT '05), pp. 227-244, 2005.
[20] 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.
[21] 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.
[22] Y. Yang, R.H. Deng, and F. Bao, "Fortifying Password Authentication in Integrated Healthcare Delivery Systems," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), pp. 255- 265, 2006.

Author Profile

Nishikant S. Burande received the B.E. degrees in Computer Science & Engineering from MBES College of Engineering Ambajogai, Dist. Beed-431517(M.S.). Persuing M.E. in Computer Engineering from Savitribai phule Pune University. Pune.