ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Efficient Co-Operative Key Exchange Protocol

K Bhoopal
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

P Manikumar
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

P Priyaraaga
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

G Deepthi
Asst professor,
Department of CSE,
TKR College of Engineering & Technology.

Abstract:

In cryptography, a password-authenticated key agreement method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password. Password authenticated key exchange (PAKE) is where two or more parties, based only on their knowledge of a password, establish a cryptographic key using an exchange of messages, such that an unauthorized party (one who controls the communication channel but does not possess the password) cannot participate in the method and is constrained as much as possible from brute force guessing the password. (The optimal case yields exactly one guess per run exchange.) Two forms of PAKE are Balanced and Augmented methods.

This paper presents the development of symmetric protocol for two-server PAKE, where the client can establish different cryptographic keys with the two servers. In addition to that a nonce will be generated during the period of authentication and this will act as a timer. If the timer does not expire with in the period limit, the authentication procedure will be carried out within the limit which provides security to replay attacks.

Keywords:

Password-authenticated key exchange, Dictionary Attacks, Diffie-Hellman Key Exchange, asymmetric protocols, Symmetric Protocols, password authentication.

Introduction:

The first successful password-authenticated key agreement methods were Encrypted Key Exchange methods described by Steven M. Bellovin and Michael Merritt in 1992. Although several of the first methods were flawed, the surviving and enhanced forms of EKE effectively amplify a shared password into a shared key, which can then be used for encryption and/or message authentication. The first provably-secure PAKE protocols were given in work by M. Bellare, D. Pointcheval, and P. Rogaway (Eurocrypt 2000) and V. Boyko, P. MacKenzie, and S. Patel (Eurocrypt 2000).

These protocols were proven secure in the so-called random oracle model (or even stronger variants), and the first protocols proven secure under standard assumptions were those of O. Goldreich and Y. Lindell (Crypto 2001)which serves as a plausibility proof but is not efficient, and J. Katz, R. Ostrovsky, and M. Yung (Eurocrypt 2001) which is practical. The first password-authenticated key retrieval methods were described by Ford and Kaliski in 2000.

Existing System:

Earlier password-based authentication systems transmitted a cryptographic hash of the password over a public channel which makes the hash value accessible to an attacker. When this is done, and it is very common, the attacker can work offline, rapidly testing possible passwords against the true password's hash value. Studies have consistently shown that a large fraction of user-chosen passwords are readily guessed automatically.

Disadvantage:

The hash value accessible to an attacker.The attacker can work offline, rapidly testing possible passwords against the true password's hash value.

Proposed System:

Recent research advances 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. In general, current solutions for password based authentication follow two models. The first model, called PKI-based model, assumes that the client keeps the server's public key in addition to share a password with the server. In this setting, the client can send the password to the server by public key encryption. Gong et al. were the first to present this kind of authentication protocols with heuristic resistant to offline dictionary attacks, and Halevi and Krawczyk were the first to provide formal definitions and rigorous proofs of security for PKI-based model.

The second model is called password-only model. Bellovin and Merritt were the first to consider authentication based on password only, and introduced a set of so-called "encrypted key exchange" protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose. Formal models of security for the password-only authentication were firstgiven 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.

Advantages:

Establish a cryptographic key for secure communications after authentication.

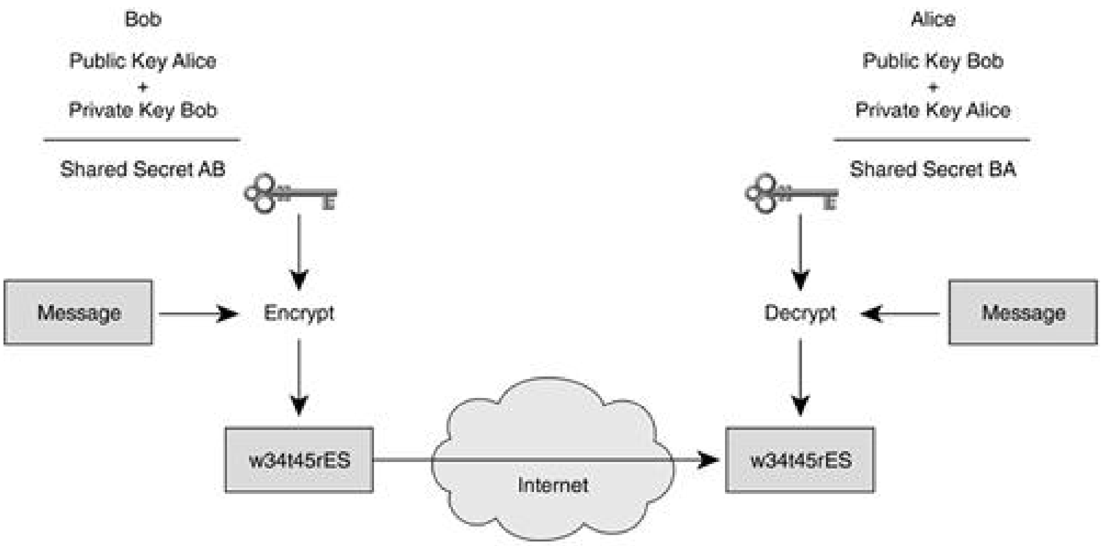
Problem Statement:

In most of existing two-server PAKE protocols such as , it is assumed or implied that the discrete logarithm of g2 to the base g1 is unknown to anyone. Otherwise, their protocols are insecure. Our initialization can ensure that nobody is able to know the discrete logarithm of g2 to the base g1 unless the two servers collude. It is well known that the discrete logarithm problem is hard, and our model assumes that the two servers never collude.The two secure channels are necessary for all two server 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.

Scope:

Our protocol provides explicit authentication in the sense that each party know that other parties have established their secret session keys correctly if the message authentication by the party succeeds. If the client C accepts the messages M4 and M5, the client C is confirmed that the servers S1 and S2 will compute their secret session keys with the client C correctly. If the server S1 accepts the message M6, the server S1 is confirmed that the client C has computed the same secret session key SK1, and the client C and the server S2 have established their secret session key correctly.

Architecture:



MODULES:

1.Diffie-Hellman Key Exchange Protocol .

2.ElGamal Encryption Scheme .

3. Initialization.

4.Registration.

Modules 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 .

4.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.

Conclusion:

The paper presents a symmetric protocol for two server password only authentication and key exchange. Security analysis has shown that the protocol is secure against passive and active attacks in case that one of the two servers is compromised the intruder cannot find out the password. Performance analysis has shown that the protocol is more efficient than current symmetric and asymmetric two server PAKE protocols in terms of parallel computation. In addition to the efficiency the authentication and key exchange should be completed within a time limit. Hence, the protocol is secure against replay attacks.

REFERENCES:

1. XunYi, San Ling, and Huaxiong WangEfficient Two-Server Password-Only Authenticated Key Exchange IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013.

2 Kyung-kug Kim, "An Improved Anonymous Authentication and Key Exchange Scheme", Proceedings of the CUBE International Information Technology Conference, pp. 740-743, 2012.

3. M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CTRSA), pp. 191-208, 2005.

4. 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.

5. 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.

6. 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.

7. 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.

8. D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586-615, 2003.

9. D. Boneh, "The Decisional Diffie-Hellman Problem," Proc. Third Int'l Algorithmic Number Theory Symp., pp. 241-250, 1998.

10. 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.

11. 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.

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

13 J. Katz and V. Vaikuntanathan "Password-based Authenticated Key Exchange Based on Lattices", In Advances in Cryptology, volume 5912 of LNCS, pp. 636–652. Springer, 2009.

14 M. Saeed, H.S. Shahhoseini, "APPMA - An Anti-Phishing Protocol with Mutual Authentication", Proceedings of the 15th IEEE Symposium on Computers and Communications (ISCC20 10), pp. 308-313, June. 2010