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

# Symmetric System for Two-Server Password-Authenticated Key Exchange

**Bheemarasetty Tinku**
M.Tech Software Engineering,
Department of Computer Science Engineering,
Vitam College of Engineering, Visakhapatnam.

**Bose Babu, M.Tech**
Assistant Professor,
Department of Computer Science Engineering,
Vitam College of Engineering, Visakhapatnam.

## \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.In this paper two servers cooperate to authenticate a client and if one server is cooperated, the attacker still cannot act as a client with the evidence from the conceded server. Current solutions for two servers PAKE are either symmetric in the way that the two server correspondingly contribute to the authentication or asymmetric in the sense that one server confirms the authenticity of legal client with the assistance of another server. 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.

## Keyword:
PAKE, Passwords, Authentication, Key exchange, Servers, Cryptographic keys.

## Introduction:

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which is to be kept secret from those not allowed access. The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword, and would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online. Passwords are vulnerable to interception (i.e., "snooping") while being transmitted to the authenticating machine or person. If the password is carried as electrical signals on unsecured physical wiring between the user access point and the central system controlling the password database, it is subject to snooping by wiretapping methods. If it is carried as packeted data over the Internet, anyone able to watch the packets containing the logon information can snoop with a very low probability of detection. Using client-side encryption will only protect transmission from the mail handling system server to the client machine. Previous or subsequent relays of the email will not be protected and the email will probably be stored on multiple computers, certainly on the originating and receiving computers, most often in clear text. Unfortunately, there is a conflict between stored hashed-passwords and hash-based challenge-response authentication; the latter requires a client to prove to a server that they know what the shared secret (i.e., password) is, and to do this, the server must be able to obtain the shared secret from its stored form. On many systems (including Unix-type systems) doing remote authentication, the shared secret usually becomes the hashed form and has the serious limitation of exposing passwords to offline guessing attacks. In addition, when the hash is used as a shared secret, an attacker does not need the original password to authenticate remotely; they only need the hash.

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

Password-authenticated key agreement generally encompasses methods such as:
•Balanced password-authenticated key exchange
•Augmented password-authenticated key exchange
•Password-authenticated key retrieval
•Multi-server methods
•Multi-party methods
In the most stringent password-only security models, there is no requirement for the user of the method to remember any secret or public data other than the password.

## RELATED WORK:

In 2011, Maryam Saeed has suggested a new two party authentication protocol without the server's public key in which the limitations of PAKE1 and PAKE2 protocols has been overcome and new authentication protocols has been implemented which can provide several security attributes while it has a remarkable computational efficiency and lower number of rounds [2]. In [2], it is proved that the Hitchcock et al.'s protocol is vulnerable to ephemeral key compromise impersonation, off-line dictionary and Key Compromise Impersonation (KCI) attacks while it does not provide the mutual authentication and forward secrecy attributes. It is also shown that SPAKEI and SPAKE2 protocols are vulnerable to password compromise impersonation and Denial-ofService (DoS) attacks while they do not provide the mutual authentication property. To remove the above disadvantages, an efficient secure two-party PAKE protocol is designed to provide several securities attributes while the efficiency is also improved. In 2010 Songs proposed very recently a password-based authentication and key establishment protocol using smart cards which attempts to solve some weaknesses [1] found in a previous scheme suggested by Xu, Zhu, and Feng [3]. In 2009, Lee et al. showed that Juang et al.'s scheme is not secure against stolen-verifier attack. Moreover, Juang's scheme does not satisfy the user anonymity. To solve this problem, Kyung-kug Kim proposed an improved anonymous authentication and key exchange scheme. Then, we show that the proposed scheme is secure against various well-known attacks [4]. In 2011 a password based authentication using Elliptic Curve Cryptography (ECC) for smart card. Since the secret key of the AS is a long-term key, it requires further security. When the secret key of the AS is compromised, the entire operation of the AS will be disrupted. Is it necessary to replace or alter the long term secret key [5]. Password-authenticated secret sharing (PASS) schemes, first introduced by Bagherzandi et al. at CCS 2011, allow users to distribute data among several servers so that the data can be recovered using a single human-memorizable password, but no single server (or even no collusion of servers up to a certain size) can mount an off-line dictionary attack on the password or learn anything about the data. Further in 2012 present a concrete 2PASS protocol and prove that it meets our definition. Given the strong security guarantees, our protocol is surprisingly efficient: in its most efficient instantiation under the DDH assumption in the random oracle model [6].In 2011 the TW-KEAP is an efficient protocol for sharing a session key to protect communication in an insecure network. It is based on the concept of the Diffie-Hellman key exchange protocol which allows the key exchange without session key appearing in the message. The TW KEAP could support lawful interception because the corresponding server is involved in the key exchange procedure to derive the session key [7].In 2012 a simple and intuitive model for expressing the semantics of privacy-friendly authentication and accountability technologies such as anonymous credentials systems and verifiable encryption. It allows for expressing the precise relations as well as the authentication and accountability properties between parties. The concepts cover in the model comprises pseudonyms, attribute-based authentication, as well as conditional release of information. As a result, the model can express the relevant primitives for privacy-preserving authentication and accountability at the same time [8].

## Existing System:

Earlier password-based authentication systems transmitteda cryptographic hash of the password over a publicchannel which makes the hash value accessible to anattacker. When this is done, and it is very common, theattacker can work offline, rapidly testing possible passwordsagainst the true password's hash value. Studies haveconsistently shown that a large fraction of user-chosenpasswords are readily guessed automatically.

## Disadvantage:

The hash value accessible to anattacker. Theattacker can work offline, rapidly testing possible passwordsagainst the true password's hash value.

## Proposed System:

Recent research advances in password-based authenticationhave allowed a client and a server mutually

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

toauthenticate with a password and meanwhile to establish a cryptographic key for secure communications afterauthentication. In general, current solutions for password-based authentication follow two models. The first model, called PKI-based model, assumes thatthe client keeps the server's public key in addition to share apassword with the server. In this setting, the client can sendthe password to the server by public key encryption. Gonget al. were the first to present this kind of authentication protocols with heuristic resistant to offlinedictionary attacks, and Halevi and Krawczyk were thefirst to provide formal definitions and rigorous proofs ofsecurity for PKI-based model. The second model is called password-only model.Bellovin and Merritt were the first to considerauthentication based on password only, and introduced aset of so-called "encrypted key exchange" protocols, wherethe password is used as a secret key to encrypt randomnumbers for key exchange purpose. Formal models ofsecurity 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-onlyauthentication protocol which is both practical and provablysecure under standard cryptographic assumption.

## Advantages:

Establish a cryptographic key for secure communications afterauthentication.

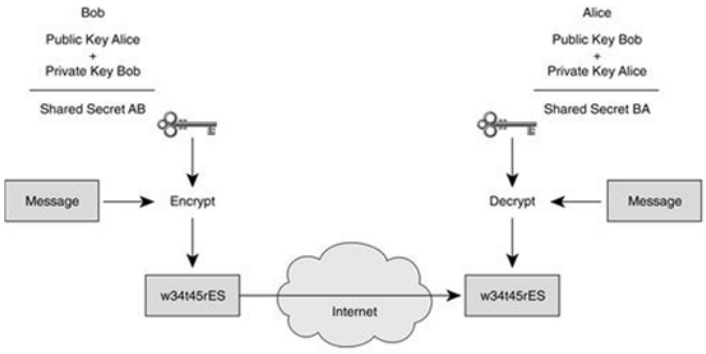
## Problem Statement:

In most of existing two-server PAKE protocolssuch as , it is assumed or implied that the discrete logarithm of g2 to the base g1 is unknown toanyone. Otherwise, their protocols are insecure. Ourinitialization can ensure that nobody is able to know thediscrete logarithm of g2 to the base g1 unless the twoservers collude. It is well known that the discretelogarithm problem is hard, and our model assumes thatthe two servers never collude. The two secure channels are necessary for all twoserverPAKE protocols, where a password is split intotwo parts, which are securely distributed to the twoservers, respectively, during registration. Although werefer to the concept of public key cryptosystem, theencryption key of one server should be unknown toanother server and the client needs to remember apassword only after registration.

## Scope:

Our protocol provides explicit authentication in thesense that each party know that other parties haveestablished their secret session keys correctly if the messageauthentication by the party succeeds. If the client C acceptsthe messages M4 and M5, the client C is confirmed that theservers S1 and S2 will compute their secret session keyswith the client C correctly. If the server S1 accepts themessage M6, the server S1 is confirmed that the client Chas computed the same secret session key SK1, and theclient C and the server S2 have established their secretsession 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 inventedby Diffie and Hellman in 1976. It was the first practicalmethod for two users to establish a shared secret key over anunprotected communications channel. Although it is anonauthenticated key exchange protocol, it provides thebasis for a variety of authenticated protocols. Diffie-Hellmankey exchange protocol was followed shortly afterward byRSA, 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

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

## 3.Initialization:

The two peer servers S1 and S2 jointly choose a cyclic groupG of large prime order q with a generator g1 and a securehash function H : {0; 1}*->Zq, which maps a message ofarbitrary length into an l-bit integer, where l= log2 q. Next,S1 randomly chooses an integer s1 fromZq and S2randomly chooses an integer s2 from Zq , and S1 and S2exchange g1s1 and g1s2 . After that, S1 and S2 jointly publishpublic 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 intotwo parts, which are securely distributed to the twoservers, respectively, during registration. Although werefer to the concept of public key cryptosystem, theencryption key of one server should be unknown toanother server and the client needs to remember apassword only after registration.

## CONCLUSION:

In this paper, we have presented a symmetric protocol fortwo-server password-only authentication and key exchange.Security analysis has shown that our protocol issecure against passive and active attacks in case that one ofthe two servers is compromised. Performance analysis hasshown that our protocol is more efficient than existingsymmetric and asymmetric two-server PAKE protocols.

## References:

[1]. Xun Yi, San Ling, Hauxiong Wang, “Efficient Two-Server Password Only Authenticated Key Exchange”, IEEE Transactions on Paralleland Distributed Systems,24,no.9, Sep. 2013.

[2]. J. Katz,P.MacKenzie,G.Taban, andV.Gligor, “Two-ServerPassword-Only Authenticated Key Exchange,” Proc. AppliedCryptographyandNetworkSecurity(ACNS’05),pp. 1-16,2005.

[3]. Y.Yang, R.H. Deng, and F.Bao,“A Practical Password-Based Two-Server AuthenticationandkeyExchangeSystem,” IEEE Trans DependableandSecureComputing, vol.3,no.2,pp. 105-114, Apr.2006.

[4].H.Jin,D.S.Wong, andY. u,“AnEfficientPassword-OnlyTwo- Server AuthenticatedKey Exchange System,” Proc.Ninth Int’l Conf.InformationandComm. Security(ICICS’07),pp. 44-56,2007.

[5].D. Jablon, “Password AuthenticationUsing Multiple Servers,”Proc.Conf.TopicsinCryptology: TheCryptographer’sTrackatRSA (RSA-CT’01),pp. 344-360,2001.

[6].P.Mackenize,T.Shrimpton,and M.Jakobsson, “Threshold PasswordAuthenticated key Exchange,” Proc.22ndAnn. Int’l CryptologyConf.(Crypto’02),pp. 385-400,2002.

[7].M. Di Raimondoand R.Gennaro,“Provably SecureThresholdPassword Authenticated Key Exchange,”Proc.22ndInt’l Conf.TheoryandApplicationsofCryptographic Techniques(Eurocrypt’03)pp. 507-523,2003.

[8].W. DiffieandM.E. Hellman, “New Directions in Cryptography,”IEEETrans.Information Theory,IT-22,no. 6,pp. 644-654, Nov.1976.

[9]. K Bhoopal, P Manikumar, P Priyaraaga& G Deepthi, Efficient Co-Operative Key Exchange Protocol, IJMETMR, Volume No: 2 (2015), Issue No: 4 (April), http://www.ijmetmr.com/olapril2015/KBhoopal-PManikumar-PPriyaraaga-GDeepthi-70.pdf

[10]. T.ElGamal, “APublicKeyCryptosystemandaSignatureSchemeBasedonDiscreteLogarithms,”IEEETrans.InformationTheory, vol.IT-31,no.4,pp. 469-472,July1985.