ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Improving Service credibility in Password Authenticated Peer Services

Vignesh.R[1], Karthikeyan.C[2], Satheesh.K[3]

M.E, Department of CSE, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India[1]
M.E, Department of CSE, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India[2]
M.E, Department of CSE, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India[3]

ABSTRACT: Two server password-based authentication protocols (Two-Server PAKE), where two servers co-operate to authenticate a client on the basis of Password only and if one server is compromised due to Insider Attack or Denial Of Service Attack (DDOS), the attackercannot pretend to be the client with the information from the compromised server. Recent research advances in password-based authentication and 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.The second model is called password-only model which follows encrypted key exchange (EKE) protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose.A password only authentication protocol which is both practical and provably-secure under cryptographic assumption.Our Protocol is Symmetric and, can run in parallel to establishes secret session keys between the client and two servers, respectively. In case one of the two servers shuts down due to the denial-of service attack, another server can continue to provide services to authenticated clients. In terms of parallel computation and reliable service, a symmetric protocol is superior to an asymmetric protocol.

Keywords:Password Authenticated Key Exchange, ElGamal encryption, Diffie-Hellman key exchange,Dictionary attack.

I.INTRODUCTION

Two server password-based authentication protocols(Two-Server PAKE), where two servers co-operate to authenticate a client on the basis of Password Only[4] and if one server is compromised due to Insider Attack or Denial Of Service Attack (DDOS). Recent research advances in password-based authentication and follow two models.A password-only authentication protocol, which is both practical and provably-secure under standard cryptographic assumption. Our Protocol is Symmetric and, can run in parallel to establishes secret session keys between the client and two servers, respectively. In case one of the two servers shuts down due to the denial-of service attack, another server can continue to provide services to authenticated clients. In terms of parallel computation and reliable service, a symmetric protocol is superior to an asymmetric protocol.We also propose a secure authentication scheme toauthenticate a client,in the scenario where two Peer servers co-operate for Authentication and if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server. Because No Password Information will be stored and keeps providing services instead of any Crash Report.Our Two-Server PAKE protocol is Symmetric, and runs in parallel in authenticating a client by Encrypted Key Exchange(EKE), providing efficient services to user.

The old password-based authentication systems transmitted a cryptographic hash of the password over a public channel which makes the hash value accessible to an attacker.It is very commonthe attacker can work offline, rapidly testing possible passwords against the true password's hash value.Keys exchange protocols are cryptographic primitives used to provide a pair of users communicating over a public unreliable channel with a secure session key. One communication round has several levels of key exchange protocols, each with its own benefits and drawbacks. An example of a popular one is the SIGMA protocol used as the basis for the signature-based modes of the Internet Key Exchange (IKE) protocol. The setting in which we are interested in this paper is the 2-party symmetric one, in which every pair of users share a secret key.

II. RELATED WORK

In [1]Liqun Chen had proposed the use of an authenticated key exchange protocol to establish a session key such that two users can securely transmit information from one domain to another. In the above scenarios a user is typically registered to some kind of domain server, such as email exchange server or home location register (in the cases of email and mobile phone communications, respectively). Moreover, two communicating parties from different domains very often neither share a password nor possess each other's public key certificate. The advantages are secure communication between two users from different administrative or security domains and4PAKE seems to be applicable to many cross-domain authenticated key exchange scenarios.The various limitation in this paper are generic protocol is understandably less efficient than one that is based on a standard. In [2] Michel had proposed a Simple Password-Based Encrypted Key Exchange Protocol.The problem identified in this paper is the related-key attacks by using a single instance of a random oracle in the key derivation process.The solution for this attack is a two new password-based encrypted key exchange protocols, called SPAKE1 and SPAKE2, both of which can be proven secure based on the hardness of the computational Die-Hellman problem in the random oracle model. The various advantages of this new technique are Minimizing the use of random oracles and Protecting against related key attacks.The limitation of this paper is the proof of security for both protocols is in the random oracle model and based on hardness of the computations. Moreover, two communicating parties from different domains very often neither share a password nor possess each other's public key certificate. Hence, although two-party and three-party authenticated key exchangeprotocols have been extensively studied and widely deployed in the real world, see for example, it is not clear how they can be directly applied to establish a secure cross-domain communication channel.Our concern here is on secure communication between twousers from different administrative or security domains.

A.DIFFIE-HELLMAN KEY EXCHANGE PROTOCOL:

This is a exactmethod of exchanging keys.
In that one of the earliest examples of Key exchange implementation in the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no previous knowledge of each other to jointly establish a shared secret key over acommunications is an insecure. This key can be used to encrypt subsequent communications using a symmetric keycipher. It is a type of key exchange. Although Diffie–Hellman key agreement itself is an *anonymous*(non-*authenticated*) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes.

B.ELGAMAL ENCRYPTION SCHEME:

ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption.ElGamal encryption can be defined over any cyclic group*G*.

III.SYSTEM DESIGN

A.SYSTEM ARCHITECTURE

The architecture design explain the overall flow of the system.It explain a new symmetric TwoServer PAKE protocol which supports two servers to compute in parallel and meanwhile keeps efficiency for practical use. Our protocol needs only four communication rounds for the client and two servers mutually to authenticate and simultaneously to establish secret session keys. In our protocol, we provide one server S1 with an encryption of the password E(g2^pw, pk2), and another server S2 with an encryption of the password E(g2^pw, pk1), where pk1 and pk2 are the encryption keys of Server1 and Server2, respectively. In addition, two servers are provided random password shares b1 and b2 subject to b1 Ex-or b2 = H(pw), where H is a hash function. The password pw is secret unless the two servers collude.

Prior to authentication, each client *C* chooses a password pwCand generates the password authentication information Auth(1) and Auth(2) for Server1 and Server2, respectively, such that nobody can determine the password pwCfrom Auth(1) or Auth(2) unless S 1 and S 2 collude.The client sends Auth(1) and Auth(2) to Server1 and Server2, respective, through different secure channels during the client registration. After that, the client remembers the password only, and the two servers keep the password authentication information. Like all existing solutions for two-server PAKE, we assume the two servers never collude in order to reveal the password of the client.An adversary in our system is either passive or active.We consider both online dictionary attack, where an attacker attempts to login repeatedly, trying each possible password, and offline dictionary attack, where an adversary derives information about the password from observed transcripts of log sessions. The online dictionary attack cannot be prevented by cryptographic means but can be easily detected and suspended once the authentication fails several times.

`B.MODULE DESIGN

1. System Initialization

The two peer servers S1 and S2 jointly choose a cyclic group G of large prime order q with a generator g1 .Next, S1 randomly chooses an integer s1 from Z* q and S2 randomly chooses an integer s2 from Z * q , and S1 and S2 exchange g1^s1 and g1^s2 . After that, S1 and S2 jointly publish public system parameters G, q, g1, g2 ,whereg2 = g^s1s2 .

2. Secret Key Establishment

The J2EE Environment is setup and Two Peer Servers are initialized and release the public parameters for the user by exchange of keys using Diffe-Helman key Exchange.The Secret key is established between Two Servers for further secure communication for Peer Servers.The Secret Session key will ensure that the two servers are Genuinely involved in the process of User Registration and Authentication to provide Peer Services for the Genuine User.Our protocol runs in three phases - initialization, registration and authentication. Of Which Initialization comes Under Secret Key Establishment which uses Diffe-Helman key Exchange.

3. User Registration

The public parameters released by Peer Servers will be used by client Registration Process, while a user registering to the Peer Services for Encryption of Password Shares and providing Authentication Information to Server 1 and Server 2 Respectively. Registration andAuthenticated Key Exchange are the Next Two Phases of our Protocol.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. Prior to authentication, each client C is required to register both S1 and S2 through different secure channels. First of all, the client C generates decryption and encryption key pairs (xi, yi) where yi= g1^xi 1 for the server Si (i= 1, 2) using the public parameters published by the two servers.Next, the client C chooses a password pwCand encrypts the password using the encryption key y, according to El- Gamalencryption.At last, the client C delivers the password authentication information Auth(1) C = {x1, a1, b1, E(g2^pwC, y2)} to S1 through a secure channel, and the password authentication information Auth(2) C = {x2, a2, b2, E(g2^pwC, y1)} to S2 through another secure channel. After that, the client C remembers the password pwConly.

4. Authentication for Peer Services DDOS Resistance

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. Prior to authentication, each client C is required to register both S1 and S2 through different secure channels. First of all, the client C generates decryption and encryption key pairs (xi, yi) where yi= g1^xi 1 for the server Si (i= 1, 2) using the public parameters published by the two servers. Next, the client C chooses a password pwCand encrypts the password using the encryption key y, according to El-Gamal encryption. At last, the client C delivers the password authentication information Auth(1) C = {x1, a1, b1, E(g2^pwC, y2)} to S1 through a secure channel, and the password authentication information Auth(2) C = {x2, a2, b2, E(g2^pwC, y1)} to S2 through another secure channel. After that, the client C remembers the password pwConly.

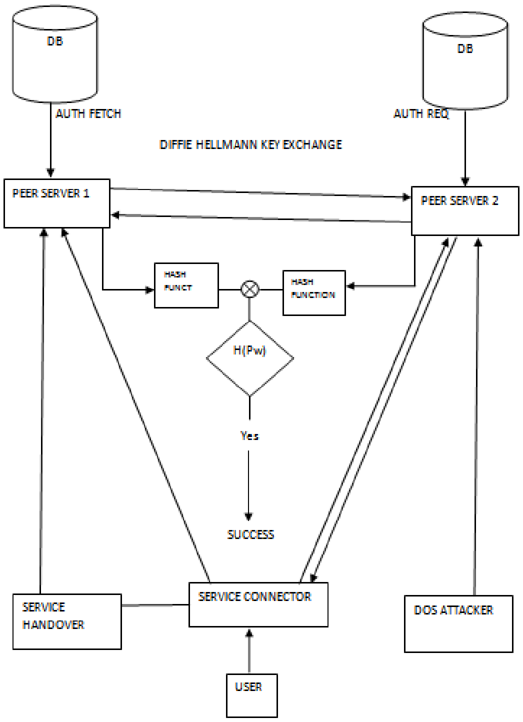
Authentication and Key Exchange:

The two servers S1 and S2 have received the password authentication information of a client C during the registration.The following steps are involved in the process of Authentication.

1.The client C randomly chooses an integer r from Z *q , computes R = g1 ^ r * g 2 ^ −pwC and then broadcasts a request message M1 = {C,Req,R} to the two servers S1 and S2

2. The Diffe-Helman Key Exchange Occurs between Peer Servers Which run in parallel and establishes a secret session to fetch the password authentication Information and the two servers mutually generate two values and send Hash functions to Client based on their Password Authentication Information's.

3. The client computes the Hash functions sent and Ex-oring the Hashes will produce the Hash of his own Password. If the Password Hash and computed Hash are same the cli8ent can ensure that he is connected with Genuine Servers and can continue enjoying Services from Peer Servers without worry.



4. The user needs to remember the Password Only. Not anything else. He is safe and secure under our Proposed Model.

IV.DISCUSSION

Most of the existing password systems were designed over a single server, where each user shares a password or some password verification data with a single authentication server. These systems are essentially intended to defeat offline dictionary attacks by outside attackers and assume that the server is completely trusted in protecting the user password database. Unfortunately, attackers in practice take on a variety of forms, such as hackers, viruses, worms, accidents, misconfigurations, and disgruntled system administrators. As a result, no security measures and precautions can guarantee that a system will never be penetrated. Once an authentication server is compromised, all the user passwords or PVD fall in the hands of the attackers, who are definitely effective in offline dictionary attacks against the user passwords.

Two server password-based authentication protocols(Two-Server PAKE), where two servers co-operate to authenticate a client on the basis of Password Only and if one server is compromised due to Insider Attack or Denial Of Service Attack (DDOS), the attacker still cannot pretend to be the client with the information from the compromised server. Recent research advances in password-based authentication and 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.The second model is called password-only model which follows encrypted key exchange (EKE) protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose. A password-only authentication protocol which is both practical and provably-secure under standard cryptographic assumption. Our Protocol is Symmetric and, can run in parallel to establishes secret session keys between the client and two servers, respectively. In case one of the two servers shuts down due to the denial-of service attack, another server can continue to provide services to authenticated clients. In terms of parallel computation and reliable service, a symmetric protocol is superior to an asymmetric protocol.

V.IMPLEMENTATION

A password authentication and key exchange protocols upon the two server model is presented in this project. It's a two-server password system in which one server exposes it to users and the other is hidden from the public. The two server model performs to be a sound model for the real applications. This method is fully depends on Key-Exchange system because the public created for the user and the service server is shared between user and service. In such architecture, the control server and the service servers are managed in different administrative domains, and the domain where the control server resides enforces more stringent security measurements. 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. This will used to keep the system more secure.

VI.CONCLUSION

A password-based authentication and key exchange system is proposed that is built upon a novel two-server model, where only one server communicates to users while the other server stays transparent to the public. Compared with previous solutions, proposed system possesses many advantages, such as the elimination of a single point of vulnerability, avoidance of PKI, and high efficiency. In contrast to existing multi server password systems, the proposed system has great potential for practical applications. It can be directly applied to fortify existing standard single-server password applications, e.g., FTP and Web applications. It can also be applied in the federated enterprise setting, where a single control server supports multiple service servers.

REFERENCES

[1] Liqunchen, hoonweilim, guomin yang, "cross-domain password-based authenticated key exchange revisited", 2013 proceedings ieeeinfocom

[2] M. Abdalla, o. Chevassut, and d. Pointcheval, "simple password-based encrypted key exchange protocols", an extended abstract of this work appears in topics in cryptology { ct-rsa 2005 (14 { 18 february 2005, san francisco, ca) a. J. Menezes ed., springer- verlag, lncs 3376, pages 191{208}

[3] Ji young chun, jungyeonhwang, dong hoon lee," authenticated key exchange secure against dictionary attacks,"ieee transactions on wireless communications, vol. 8, no. 5, may 2009.

[4] Hasennicanfar, *student member, ieee, and victor c. M.leung, fellow, ieee.* Multilayer consensus ecc-based password authenticated key-exchange (mcepak) protocol for smart grid system. Ieee transactions on smart grid, vol. 4, no. 1, march 2013 253.

[5] 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.

[6] Xunyi, san ling, and huaxiongwang, "efficient two-server password-only authenticated key exchange", ieee transactions on parallel and distributed systems, vol. 24, no. 9, september 2013.

[7] Ji young chun, jungyeonhwang, dong hoon lee, "a note on leakage-resilient authenticated key exchange"ieee transactions on wireless communications, vol. 8, no. 5, may 2009.