International Journal of Soft Computing 9 (5): 355-358, 2014
ISSN: 1816-9503

Multi-Server Password-Only Authenticated Key Exchange in Diffie-Hellman Key and ElGamal Encryption Algorithm

[1]S. Raghavendran, [1]P. Darwin, [1]P. Dayakar Rao,
[1]B. Senthil Kumaran and [2]K.V. Vijayasekaran
[1]Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Vel Tech Dr. R.R and Dr. S.R Technical University, Avadi, Chennai, India
[2]Vel Tech Multitech Dr. Rangarajan Dr. Sakuntala Engineering College, Avadi, Chennai, India

Abstract: A networks system can solve computational problems it can coordinate the use of shared resources or data and also provide communication services to client and server. In network client server communication who shares the password, check the process of communication between them and meanwhile establish a cryptographic key by exchange of messages and information. A client will store a password mutually in the one server and If that server failed for authentication, the unauthorized access may happen. In this study, researchers consider two servers cooperate to authenticate a client and if one server is failed for authentication, the attacker still cannot access the client information from the failed or compromised server. A two server password authenticated key exchange is parallel in the manner that two peer server equally put up to for the authentication.

Key words: Diffie-Hellman key exchange, password-authenticated key exchange, ElGamal encryption, dictionary attack, networks

INTRODUCTION

The Client-Server Model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers and service clients. The client-server characteristic describes the relationship of cooperating programs in an application. The server component provides a function or service to one or many clients which initiate requests for such services. A shared resource may be any of the server computer's software and electronic components from programs, data to processors and storage devices. The sharing of resources of a server constitutes a service. The client and server communicate through the network by separate hardware and it is reside in the same peer. In cryptography, a Password-Authenticated Key Agreement (PAKE) (Juang, 2004; Zhang *et al*., 2014). Method is method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password.

A secure communication over insecure open networks has been a great concern for researchers. During recent years, cryptographic approaches have been applied to remove these problems. Among these approaches, Password Authenticated Key Exchange (PAKE) protocols have been played an essential role in providing secure communications. PAKE protocols permit a client and a server to authenticate each other and generate a strong common session key through a pre-shared human memorable password over an insecure channel. Two-party password-based authenticated key exchange protocol is quite useful for client-server architectures. However, in large-scale client-client communication environments where a user wants to communicate with many other users, Two-PAKE protocol is very inconvenient in key management that the number of passwords that the user would need to remember. Security in computers is information protection from unauthorized or accidental disclosure while the information is in transmission and while information is in storage. Authentication protocols provide two entities to ensure that the counterparty is the intended one whom he attempts to communicate with over an insecure network. These protocols can be considered from three dimensions: type, efficiency and security.

In general, there are two types of authentication protocols, the password-based and the public-key based. In a password based protocol (Kwon *et al*., 2005), a user

Corresponding Author: S. Raghavendran, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Vel Tech Dr. R.R and Dr. S.R Technical University, Avadi, Chennai, India

registers his account and password to a remote server. Later, he can access the remote server if he can prove his knowledge of the password. The server usually maintains a password or verification table but this will make the system easily subjected to a stolen-verifier attack. To address this problem, recent studies suggest an approach without any password or verification table in the server. Moreover, to enhance password protection, recent studies also introduce a tamper-resistant smart card in the user end. In a public key-based system, a user should register himself to a trust party, named KGC (Key Generation Center) to obtain his public key and corresponding private key. Then, they can be recognized by a network entity through his public key. To simplify the key management an identity-based public key cryptosystem is usually adopted in which KGC issues user is ID as public key and computes corresponding private key for a user. Attackers easily eavesdrop, modify or intercept the communication messages on the open network. Hence, an authentication protocol should withstand various attacks such as password guessing attack, replay attack, impersonation attack, insider attack and man in the middle attack. Considering computational efficiency in an authentication protocol in this study, researchers analysis about more secure message communication using the Diffie-Hellman key exchange and ElGamal encryption techniques.

DIFFIE-HELLMAN KEY EXCHANGE

The Diffie-Hellman algorithm (Yi *et al*., 2013; Jeong *et al*., 2007) was the first Public Key algorithm eves invented in the year 1976. In this protocol method, the two nodes that have to communicate in the unsecure channel and establish a secrete key without prior knowledge between them. The secrete key can be used for encrypt communication using Symmetric Method.

Diffie-Hellman algorithm (Harn *et al*., 2004) allows two users to communicate with each other to obtain a secure key in the public communication channel.

Researchers consider two uses have Alice and Bob, the attacks will attack by eavesdropping the messages by both Alice and Bob is unable to determine the shared secret key.

This is important because the shared secret can be used to generate a secret session key that can be used with symmetric cryptosystems.

The Alice and Bob users who know nothing about each other but wish to establish secure communications between them to wish to establish secure communications between them Diffie-Hellman key exchange protocol can be used as in Fig. 1.

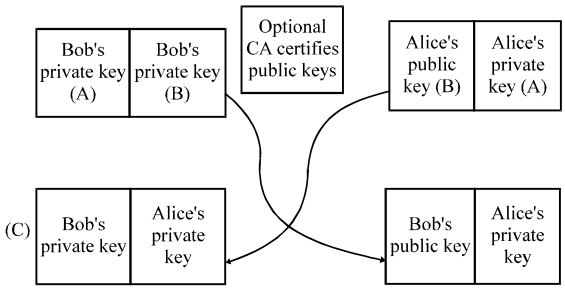

Fig. 1: Diffie-Hellman key exchange protocol

Discrete alogarithms and Diffie-Hellman: In this Alice and Bob to agree on a large prime p and non-zero integer g modulo p:

$$A = g^a \pmod p$$

$$B = g^b \pmod p$$

They next exchange these computed values, Alice sends A to Bob and Bob sends B to Alice. Finally:

$$A^1 = B^a \pmod p$$

$$B^1 = A^b \pmod p$$

The values that they compute, A^1 and B^1, respectively are actually the same, since:

$$A^1 = B^a = (g^b)^a = g^{ab} = (g^a)^b = A^b = B^1 \pmod p$$

Definition: Let P be a prime number and g an integer, the Diffie-Hellman Problem (DHP) is the problem of computing the values of $g^{ab} \pmod p$ from the known values of $g^a \pmod p$ and $g^b \pmod p$.

ELGAMAL ENCRYPTION ALGORITHM

ElGamal Encryption (Yi *et al*., 2013; Lian *et al*., 2006) algorithm is an symmetric key encryption algorithm for public key cryptography. This algorithm was developed based on Diffie-Hellman key exchange. The ElGamal Encryption algorithm consist of key generation, encryption, decryption methods, security and efficiency.

Key generation: A key generation (Tarman *et al*., 1998) is a process of generating the keys to the algorithm on input of variables or data to generate the keys and computes the encryption operation.

Encryption: An encryption is a technique which takes the plaintext and generates the cipher text according to the inputs.

Decryption: A decryption is a process of generates the plain text from cipher text. The ElGamal encryption techniques, the text message can be encrypted simultaneously it will generate different cipher text. Luo (2000) proved ElGamal Encryption Method is Secured Encryption Methods secure under the Decisional Diffie Hellman (DDH) assumption.

DUAL SERVER PASSWORD AUTHENTICATION AND KEY EXCHANGE

In this project (Yang and Yang, 2010; Luo, 2000), there will be a two severs S1, S2 and group of clients. The two servers will authenticate the client for message communication between the clients. Every Client (C) chooses the password P^C and create the password authentication AC(1) and AC(2) certificate for both the server S1 and S2. The difficulty to trace out the password PWC from AC(1) of AC(2) unless S1 and S2 collude.

The clients send the authentication to the server S1 and S2 through the communication channel for registration. The client will maintain the password only and the sever will maintain the password authentication information. The two server cooperate to maintain client information. The client transmit the message or data over the channel the two server will authenticates simultaneously, if one server failed for authenticate, the another server will coordinates the authentication. In this protocol if each server establishes a secret session key with the client.

BLOCK DIAGRAM OF THE SYSTEM

Login check: The user login into the system check whether the user is authenticated or not. The user is authenticate it will allow to communicate with other system, else it will be terminated.

Key generation: A key generation is a process of generating the keys for sender and receivers. A sender receives the key from the server and encrypts the messages and transferred to the public communication channel. A receiver receives the key from server and decrypts the messages and downloads it.

ElGammal encryption: ElGammal Methods can be classified into key generator, the Encryption algorithm and Decryption algorithm. The sender will encrypt the messages and transferred into the public channel and receiver will decrypt the information and receive it (Fig. 2).

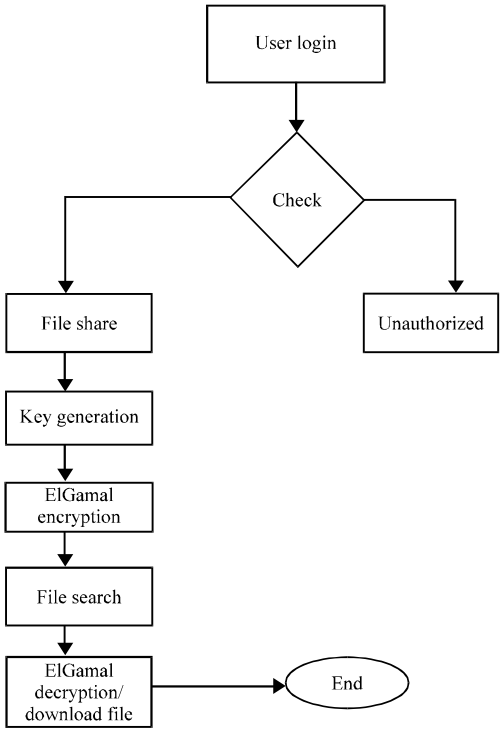

Fig. 2: Block diagram of the system

CONCLUSION

This study describes symmetric protocol for Diffie-Hellman and ElGamal algorithm for two server password only authentication in this protocol, researchers analyse the secure communication between the system when one server failed to compromised, the another server can maintain the authentication check. Performance analysis has shown that the protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols.

ACKNOWLEDGEMENT

Researchers would like to appreciate valuable comments from reviewers. These comments are really helpful for us to development of this study.

REFERENCES

Harn, L., M. Mehta and W.J. Hsin, 2004. Integrating diffie-hellman key exchange into the Digital Signature Algorithm (DSA). IEEE Commun. Lett., 8: 198-200.

Jeong, I.R., J.O. Kwon and D.H. Lee, 2007. Strong diffie-hellman-DSA key exchange. IEEE Commun. Lett., 11: 432-433.

Juang, W.S., 2004. Efficient multi-server password authenticated key agreement using smart cards. IEEE Trans. Consum. Electron., 50: 251-255.

Kwon, T., Y.H. Park and H.J. Lee, 2005. Security analysis and improvement of the efficient password-based authentication protocol. IEEE Commun. Lett., 9: 93-95.

Lian, S., Z. Liu, Z. Ren and H. Wang, 2006. Secure advanced video coding based on selective encryption algorithms. IEEE Trans. Consum. Electron., 52: 621-629.

Luo, H., 2000. A server-independent password authentication method for access-controlled Web pages. Proceedings of the IEEE Global Telecommunications Conference, Volume 1, 27 November-December 1, 2000, San Francisco, CA., pp: 361-364.

Tarman, T.D., R.L. Hutchinson, L.G. Pierson, P.E. Sholander and E.L. Witzke, 1998. Algorithm-agile encryption in ATM networks. Computer, 31: 57-64.

Yang, D. and B. Yang, 2010. A novel two-server password authentication scheme with provable security. Proceedings of the IEEE 10th International Conference on Computer and Information Technology (CIT), June 29-July 1, 2010, Bradford, pp: 1605-1609.

Yi, X., S. Ling and H. Wang, 2013. Efficient two-server password-only authenticated key exchange. IEEE Trans. Parallel Distrib. Syst., 24: 1773-1782.

Zhang, L., S. Tang and Z. Cai, 2014. Robust and efficient password authenticated key agreement with user anonymity for session initiation protocol-based communications. IET Commun., 8: 83-91.