INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 1 (2017) PAGES 1622 - 1626
RECEIVED : 15.02.2017 PUBLISHED : 26.02.2017
February 26, 2017

EFFICIENT HYBRID MULTI SERVER BASED PASSWORD AUTHENTICATION KEY PROTOCOL

Parkavi.S[1], Kalpana.N[2]
[1]PG Student, Dept. of Computer science and Engineering, Priyadarshini Engineering College, Vaniyambadi,Tamilnadu, India,
[2]Associate Professor, Dept. of Computer science and Engineering, Priyadarshini Engineering College, Vaniyambadi, Tamilnadu, India.

Abstract

Traditional Password-authenticated key exchange (PAKE) protocol involves a client and a server share a common password for authenticating each other and establishes a cryptographic key (like Diffie Hellmann key exchange) for the exchange of messages. In this all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised by a, hacker or even insider attacks, all the passwords are disclosed and the client server authentication fails. In this proposed Multi server password authentication, client splits and stores its password in two or more servers and they will cooperate with each other to authenticate a client. In this scenario, even though one server is compromised, the attacker still cannot succeed as attacker needs rest of password from other server for client server authentication. Multi server password authentication may be either symmetric in which all servers equally contribute to the authentication or asymmetric in which that one server authenticates the client with the help of other server. This paper presents a symmetric solution for the multi-server PAKE. The overall performance is improved by the parallel processing of the multi server in which all the server concurrently produces password for authenticating a client system.

Keywords: Password-authenticated key exchange (PAKE), Diffie Hellman key exchange, Multi server password authentication, Elgamal Encryption.

1. INTRODUCTION

An authenticated encryption key is required for secure communication. Two methods are used for authenticated key exchange. One method involves shared cryptographically-strong secret key used, or a public key stored in device used for encryption/authentication of messages. Another method involves human memorable password used for encryption/authentication of messages. Bellovin and Merritt [1] introduces password-based authenticated key exchange (PAKE), where two parties, establish a cryptographic key based on their knowledge for the exchange of messages. A PAKE protocol may resist the on-line and off-line dictionary attacks.

The traditional password-based authentication key is based on

Password-only PAKE: In this two parties shares a common password, they establish a common secret key by the exchange of messages encrypted by the known password [1]

PKI-based PAKE: In this the client stores the server's public key along with the password [2] .

ID-based PAKE: In the client needs to remains a server password along with the server identity. The server keeps track of password along with the private key in addition to its identity.

In single-server model, all the needed passwords to authenticate clients are stored in the single server. If it is compromised then the message will be disclosed [3]This is also applicable to Kerberos [4], where a user authenticates a authentication server using username and password and gets a token for authenticating the service server.

2. LITERATURE SURVEY

Much more techniques are used for password authentication. Public Key Info systems is one of the method that uses public key infrastructure for generating public keys to avoid password hacking. The disadvantage is user has to verify the validity of the key each and every time. it consumes more time. Then, another method known as password only protocols or Password Authenticated Key Exchange (PAKE) which uses public key system for password authentication.

2.1 Pseudo Random And Hash Password Models

Pseudo Random number generator generates a number that changes every time. Only sender and receiver knows this and it resists the online dictionary attack. Secure hash function is used for password generation. Hash function is one way with message and hash function hash code can be generated but reverse is not possible.

2.2 Server Effects in Password Systems

If the server is hacked by outside observers, then the user authentication will be exposed. The user tries to enter into the website, the application first asks for the master password. If the entry is correct, then it allows the user to enter the password. If the user tries to expose the master password, then it will allow the attackers to seize the users' confidential information.

2.3 Single Vs Multi Server

To protect the server from offline dictionary attack, single server setting was used by Gong et al (1993) in a hybrid, PKI-based model in which the users' can let to know about the servers' public key along with their password. Bellovin and Merritt (1992) were the very first to proposed protocols designed for password-only authenticated key exchange, where the clients are required to store only a short password and no additional information. The initial works by Bellovin and Merritt (1993), Jablon (1996) and Lucks (1997) were inefficient and it provides no security for the user. Recently, Bellovin and Merritt (1992), Halevi and Krawczyk (1999) followed a model for the password-only setting. Goldreich and Lindell (2001) discussed associated protocols with proofs of security in the random oracle/ideal cipher models. Gennaro and Linddell (2003), Jiang and Gong (2004) assumed some public information which is available to all parties. Since this public information is coded into implementation of protocols, it is not necessary for the user to memorize high-entropy, cryptographic information as they are required to do in the PKI-based setting.

2.4 Two Server Password

The application of this research work would be an integrating the Quantum key distribution protocol (QKDP) and classical model, in which TC and a participant synchronize their polarization bases according to a pre-shared secret key in the two server password authentication system. During the session key distribution, the pre-shared secret key combined with random string which is used to

produce an encryption key to encipher the session key. So, there is no chance for the recipients to get the same polarization quantum bits, even if an identical session key is retransmitted. The traditional public key cryptography uses some computational functions and the users will face difficulties in maintaining the information. Since Quantum cryptography uses quantum mechanisms, it provides a better security service for the users' hold into it. The quantum cryptography will transmit or distribute only a key not a message or any data. This key can then be deployed with any available encryption algorithm in order to encrypt and decrypt a message which can again be transmitted over a standard communication channel. The algorithm associated with QKD key consists of one-time pad as it is completely secured when used with a secret random key. Traditional encryption technique requires users to protect the secret key by providing it with a password. So, it is necessary for the user to remember the password or pass-phrase to get the secret key. Ellison et al (2000) proposed a scheme whereby a user can protect a secret key using the personal entropy by way of encrypting a password by answering to several questions. So, there is a chance to the user to forget the answer for the questions and the attacker may also struggle to get the answers for the questions to recover the shared secret key. Recently planned two server password systems as referenced by Yang et al (2006), Gottesman and Lo (2003) go through a model in which user can communicate with only one server and the public could not communicate to the second server. So it might be difficult for the user to use the benefits of this system.

2.5 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 our proposed solution for multi-server PAKE, the registered client will generate multiple parts of a corresponding single password such as pw=pw1+pw2+…pwn. The splitting of password is based on the number of available authentication server.

The password will get split in following way in number of servers: Consider,

V = number of characters in server 1,2,3,4 respectively,

Password= pw

Step1:- pw1 = Pw length/2 Where, If v1 < 2

then v1 = 2.

Step2:- V2 = Pw length - V1 – 4

Where, If V2 < 4 then V2 = 2

Step3:- V3 = Pwlength - V2 - V1 - 2

Step4:- V4 = Pw length - V3 - V2 - V1

This above equation will split the password into random number.

A secret session key is established between the client and different authenticating servers using Diffie Hellman key exchange let it be sk1, sk2 …skn . Diffie Hellman key exchange[6] is used to share a secret key in un secured channel. Although it is a non authenticated key exchange protocol, it provides the basis for a variety of authenticated protocols.Establish a cryptographic key for secure communications after authentication.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 1 (2017) PAGES 1622 - 1626
RECEIVED : 15.02.2017 PUBLISHED : 26.02.2017
February 26, 2017

Password registration phase

The client encrypts the multiple parts of password E_{sk1}(pw1), E_{sk2}(pw2)…. E_{skn}(pwn) and send to different servers. Each server stores the part of password and they are unknown of other server password and Elgamal encryption scheme[7] may be used encryption the passwords.

ElGamal Encryption Scheme

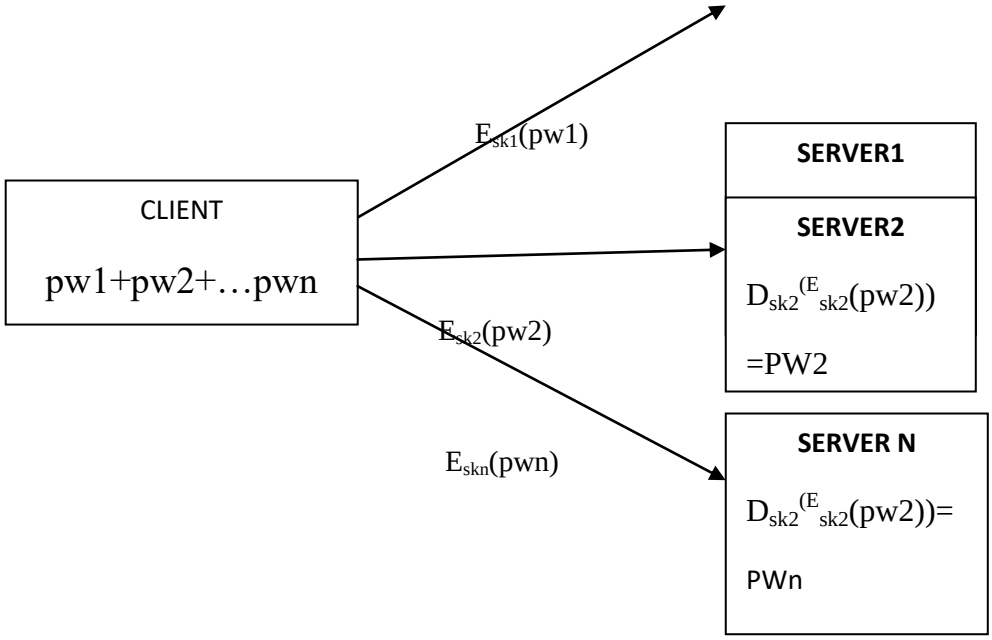
Each user has a private key x

Each user has three public keys: prime modulus p, generator g and public Y = gxmod p

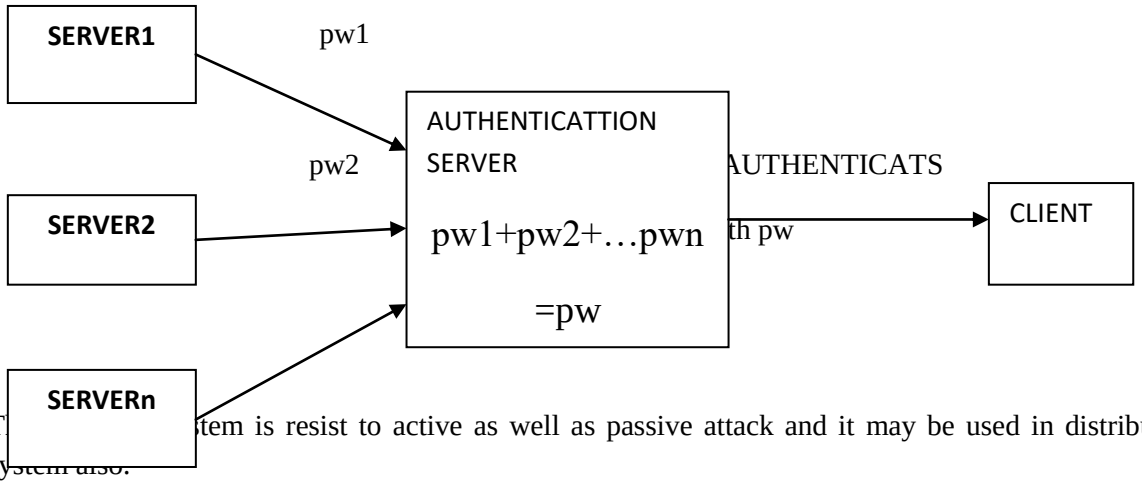
Security is based on the difficulty of DLP

Secure key size > 1024 bits (today even 2048 bits)

Elgamal is quite slow, it is used mainly for key authentication protocols



2.6 Password Retrieval Phase



T tem is resist to active as well as passive attack and it may be used in distributed system also.

CONCLUSION

In this paper, we develop a symmetric protocol for multi-server password authentication system. The proposed system is secure against passive and active attacks in case that one of the many servers is compromised. Performance analysis has shown that our proposed system is more efficient than existing symmetric and asymmetric two-server PAKE protocols

FUTURE SCOPE

The proposed paper can used with kebroes a client authenticating service which issues token for authenticating client system. More security is attained in kebroes as we use multi server password in client authentication and it may resist various form of attach. It can also be used in keberos relam where authentication server resides in another network.

REFERENCES

[1] P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer, and H. Jin, "Generating searchable public-key ciphertexts with hidden structures for fast keyword search," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1993–2006, 2015.

[2] L. Gong, T. M. A. Lomas, R. M. Needham, and J. H. Saltzer . Protecting poorly-chosen secret from guessing attacks. IEEE J. onSelected Areas in Communications, 11(5):648-656, 1993.

[3] X. Yi, R. Tso and E. Okamoto. ID-based group password-authenticated key exchange. In Proc. IWSEC'09, pages 192-211,2009

[4] B. Clifford Neuman and Theodore Ts'o. Kerberos: An authentica-tion service for computer networks. IEEE Communications, 32 (9):33-38, 1994.

[5] T.S.Thangavel and A. Krishnan Provable Secured Hash Password Authentication 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 19

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

[7] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,"IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472,July,1985.