NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 3, ISSUE2, FEB.-2016

EFFICIENT TWO-SERVER PASSWORD-ONLY AUTHENTICATED KEY EXCHANGE

Miss. Alfiya Bagwan,
BE Computer Science & Engg. Department JSPM'S BIT, Barshi

Miss. Manjusha Nawale,
BE Computer Science & Engg. Department JSPM'S BIT, Barshi

Miss. Sana Mulani,
BE Computer Science & Engg. Department JSPM'S BIT, Barshi

Miss. Priyanka Jagtap
BE Computer Science & Engg. Department JSPM'S BIT, Barshi

Guide- Prof. Kumbhar P.B.
BE Computer Science & Engg. Department JSPM'S BIT, Barshi

Special Thanks to
Dr.* Vyankatesh S. Kulkarni
Mechanical Engg. Department JSPM'S BIT, Barshi

ABSTRACT

Password-authenticated key exchange (PAKE) is placed in between client and a main server, which is used to share a password and authentication of password and in parallel establish a cryptographic key by exchanging messages. While doing these settings the entire password are stored in mainframe server. If the server is hacked or even malfunction happens due to internal system password stored will be open to hacker. This paper is written for consideration a two main servers operate in hand shake mode and one of them is hacked or malfunctioning. The advantage of this system even if one system is hacked, the hacker will not be able to see anyone's password or any other information. The proposed system proposes two servers, using password-authenticated key exchange(PAKE). In this case two servers will operate in handshake mode, and contribute to a generation of one key for authentication.
Proposed system presents a symmetric solution for two server by using PAK, where client will get access to two different servers using cryptographic keys. The protocol develops runs in parallel operation to save time, and it is found that it is more secure and efficient than existing system.

KEYWORDS— PAKE, Elgamal, Diffie-Hellman, Periodic Backup, Encryption

INTRODUCTION

The system develop has an user authentication based on PAKE and found beneficial in terms of low cost, less time consuming as it uses multitasking and most importantly ease of access. The advantage of easy to access is most appealing amongst the common people. Where user will get a advantage of

remembering a very short password, user need not to remember a very long password having alphanumeric keys. Though system develop has an short password, still it can be use anywhere, because it is genuine regardless of type of access. A password is simple terms can be written as, it is secret code comprising a word or string it can be even alphanumeric used for authentication of the user and prove the identity. Use of passwords can vary according to user application, mostly it is used for login process and for accessing computer operating systems, ATM machines and mobile phones.

A PAKE system is also used in case of computer for purposes log in and various password related activities of computer and internet. Some years back the password based authentication worked on cryptographic hash of the password using public channel which gives the possibility of hash number to an attacker. If this facility is made available to hacker, the hacker may work offline, and can generate many possibilities for generation of the password.

New trends are being develop in the password authentication have given a facility client and a mainframe server in handshake mode and meanwhile generate and cryptographic key for authentication by using PAKE. Password is only used for protocol authentication and prevents theft or hacking. The encryption and decryption key pairs is exchanged between two servers are generated by the client server and the same is delivered to other servers through secure channels. Arbitrary number or nonce is generated only one time and it is sent to the other servers during the primary phase of authentication.

The generated arbitrary number is randomly generated and won't get repeated. The server program is design in such a way that, it will keep the track of all activities. Consider, if hacker is trying to access any of the nonce. The server program is design to identify that intruder is working beneath it. The disadvantage of asymmetric two server PAKE protocol is it runs the series only for the front end server and the client need to establish a secret session key at the end. Having above stated disadvantage of asymmetric protocol, many times symmetric protocol is used for authentication.

LITERATURE REVIEW

In recent times, Katz et al. recommended the first two servers will authenticate key for exchange protocol with an proof or evidence of security in the standard model. Their protocol stretched and built upon the Katz - Ostrovsky- Yung PAKE protocol called KOY protocol. In this proposed system the client Z has choice of selecting password. Two designated server X &Y will delivered random password and PW1 and PW2 subject to condition of PW1+PW2=PWz. At some level this protocol will be a implementation of the KOY protocol, one between client Z and server X, and at this time server Y will support for confirmation of authentication. The assistance of the another server, which acts as a observer is needed as password is divided in two main servers. At the end of authentication protocol secret session key is generated between every server and the client. Symmetric protocol (KOY) is used, so that two servers will contribute for the authentication of key and exchange. The major advantage of KOY protocol is the structure of the protocol used is symmetric and hence required two servers for generation of protocol and authentication, its major disadvantage is it cannot be used practically.

Researcher yang and team suggested few other settings in asymmetric, where front end server will be called service server(SS), and this server will be used for co-operation with the client, whereas a back end server will be called control server(CS). And this helps in authentication with SS and only SS and the client will generated for at the end of every session. Yang et al carried out research in two phases in 2005 they suggested a PKI based asymmetric PAKE control and in 2006 they came up with

the idea of different kinds of asymmetric protocol. In the generated protocol the client have to initiate a request, and service server rejoins with B=B1B2 where B1= g1b1g2π1 and B2= g1b2g2π2 are created by SS and CS, this is generated on the basis of random password π1 and π2 individually, and then client can get g1(b1+b2) by eradicating the password π= π1+ π2 from B/g2π. In the next step, SS and the client will authenticate each other by verifying, whether they approve on the same secret session key, key, either g1a(b1+b2) or g1aa1(b1+b2), with the help of CS, where a, (a1, b1) and b2 are randomly chosen by the client, SS and CS, respectively. The major advantage of Yang *et al.* protocols over Katz et al is they can be used practically.
Joblon proposed the condition for PKI and implemented new type of protocol, which is related to the property in the password only model. Both type of protocols implemented above are of AKE and threshold protocols, were not much secure. In 2002, McKenzie et al. proposed protocol in the PKI based setting which facilitates only time out of any number of servers, and collaboration to authenticate a client and it is found safe for authentication. In 2003 Joblon et al are first researchers to say confidently with proof for threshold PAKE protocol in ORACLE.

PROPOSED SYSTEM

In recent years researchers have given advance technique for password authentication and have facilitated client and server mutually to authenticate with a password and at same time cryptographic key is generated after authentication.

MODELS FOR AUTHENTICATION

i) The first developed is PKI based model, requires client to keep the server's public key with already shared password with the server. The advantage of this type of setting, is the client has facility to send the password to the server by using public key encryption. This kind to password authentication first proposed by Gong and his team. This type of approach uses heuristic technique for prevention of malpractice. The two major pioneer scientists Halevi and Krawczyk were the first to provide rigorous and extensive evidence for security for PKI based model.
ii)Another type of model is only password based. Two researchers Merritt and Bellovin were the first to demonstrate concept of password only authentication. And this two scientis have developed the first to introduce concept of "encrypted key exchange". The password in this case, is nothing but is a secret key to encrypt random number for exchange of key. Though above two scientists given a fundamental concept of password only authentication but formal models of security is been only given by the Boyko et al and Bellare et al. and Katz et al.

DIFFIE-HELLMAN KEY EXCHANGE PROTOCOL.

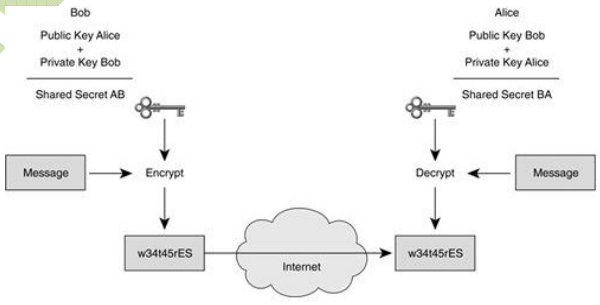

Fig 1. Working of Diffie-Hellman Key Exchange Protocol.

Author in this paper describes the implementation of a two server authentication system using the Diffie-Hellman algorithm. The disadvantage of existing Diffic-Hellman algorithm was overcome that if one server shuts down because of any reason or failure, another server will take care of a whole system is implemented in the proposed model.
Two servers (S1) and server (2) are used to keep the back up for 48hours. The advantage offered by this system that even after failure, the system will work for 48hrs without any difficulty and maintenance person will get breathing time for 48hrs.

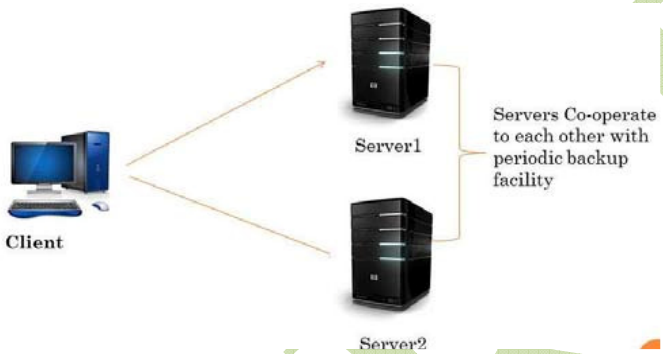

Fig 2: system architecture

Fig 2. shows about the system architecture, here two servers are there, client is authenticated by two servers only. This type of system helps in preventing dictionary attacks. As both the servers contribute equally to the system so these servers are symmetric servers.

MODULES

1. Diffie-Hellman Key Exchange Protocol.
2. El Gamal Encryption Scheme.
3. Initialization.
4. Registration.

1.Diffie-Hellman Key Exchange Protocol

This protocol for exchange of key was introduced by two great scientists Diffie and Hellman in the year 1976. They have given a practical solution for sharing a secret key between two users over unprotected communication channel. The Diffie-Hellman key exchange is non authenticated type of protocol for exchange of key. This two scientists were not successfully but they have provided the basis for many other type protocol to upcoming researchers. RSA has taken up the efforts put the by the Diffie and Hellman for first practical public key cryptosystems.

2. ElGamal Encryption Scheme

In this case security key is based on the difficulty of DLP. The security key size is greater than 1024bits. In this encryption scheme each user has a private key(X). Each user is provided with three public keys
1. Prime Modules (P)
2. Generator (g)

3. Public (Y) = Gxmod p.
This disadvantage of this type of module is quite slow and it can be only use for key authentication of protocols.

3.Initialization

Two peer servers named as S1 and S2 are used in handshake mode for choosing a cyclic group G of very large prime order Q with generator g1 and a secure has function H. {0; 1}*->Zq, which is used for mapping a message of any arbitrary length for an 1 bit integer, where 1 – log2q. In the second step server one (S1) chooses in integer from Zq in random fashion/ and in similar way Server two S2 chooses an integer number from S2 from Zq. And then program is made in such a way that S1 and S2 will exchange g1s1 and also g1s2. After completion of this operation, S1 and S2 together publishes a public system parameters G; q; g1; g2;H where g2 = gs1s2 .

4.Registration

There is necessity of two channels for implementation of two server PAKE protocols, that is the reason splitting of password is possible in two parts. The split passwords are fed to the two servers over a secured communication channel at the time of registration. In this paper concept of public key cryptosystem is preferred and implemented. In this case there will not be any communication between two servers for encryption key, in this case client needs to remember a password only after registration.

CONCLUSION

Here proposed the various PAKE protocol. Two types of servers are also explained that are symmetric and asymmetric. Diffie-Hellman and Elagamal encryption algorithms are basic building blocks of the explained protocol. Here it is important to consider that if one server shutdown due to some reason then there is facility to the servers to take periodic backup. By using periodic backup technique the redundancy in the data an be avoided. Security propose that it is very important an d efficient protocol. Mainly this protocol uses the public key encryption so that communication is done through secure channel instead of broadcasting from client to the servers. After security analysis it is come to know that this protocol secure against active and passive attack.

REFERENCES

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

[2] X. Yi, R. Tso, and E. Okamoto, "*ID-Based Group Password- Authenticated Key Exchange," Proc. Fourth Int'l Workshop Security:Advances in Information and Computer Security (IWSEC '09), pp. 192-211, 2009.*

[3] J. Katz, P. MacKenzie, G. Taban, and V. Gligor, "*Two-Server Password-Only Authenticated Key Exchange," Proc. Applied Cryptography and Network Security (ACNS '05), pp. 1-16, 2005.*

[4] J. Katz, P. MacKenzie, G. Taban, and V. Gligor, "*Two-Server Password-Only Authenticated Key Exchange," Proc. Applied Cryptography and Network Security (ACNS '05), pp. 1-16, 2005.*

[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.*