International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-3, March 2015

Password Authentication Using Two Server Key Exchange

Lekha Deshmukh, Ankita Kathale, Sayali Kulkarni, Prof. Smita Chaudhari

***Abstract*— Two server PAKE (Password Authentication Key Exchange) use symmetric solution to authenticate client in client server authentication system. This system have advantage that encrypted password get store in two server instead of single server to minimize disadvantage of single server system. Both the server communicate and exchange messages to authenticate client. OPT (One Time Password) is also a secure solution which uses random function to generate password and this password get discard after one use. In this paper, two server PAKE and OTP protocol is combine to overcome drawback of previous systems and provide more security. First two server PAKE will run to store the encrypted password in two server and then to authenticate the client OTP protocol send OTP on the client's mobile. Only using this OTP the client will get the authenticated.**

***Index Terms*— PAKE (Password Authentication Key Exchange), Key Exchange, Diffie-Hellman Key Exchange Protocol, cipher text, ElGamal encryption schema.**

I. INTRODUCTION

Passwords are one of the important factor of security which is used in day to day life for logging process into the computer system, mobile phones etc. Also along with the password importance, security of it is one of big issue. Authentication systems based on user id and password are very efficient and are low cost systems.

Previously there was single server system where all the passwords were stored which was a vulnerable system .If that server gets compromised then all passwords were disclosed. Passwords can be easily cracked because of single point failure.

Password authentication key exchange is where client and server communicate with each other using the cryptographic key. The two solutions for PAKE are symmetric and asymmetric solutions. Symmetric is where both the servers work together to authenticate the client. In Asymmetric solution one server takes the help of another server to authenticate the client. In symmetric solution both the servers and client establishes a secret key session. Asymmetric solution works in series and only client and the main server needs to establish secret key. Symmetric protocol works in parallel which makes it reliable than asymmetric system. To address the issue of single server system we are going use the concept of multiple servers.

Manuscript received March 18, 2015

Lekha Deshmukh, Computer Engineering, International Institute of Information Technology, Pune, India, 8806121712.
Ankita Kathale, Computer Engineering, International Institute of Information Technology, Pune, India, 8796539647.
Sayali Kulkarni, Computer Engineering, International Institute of Information Technology, Pune, India, 7743824634.
Prof. Smita Chaudhari, Assistant Professor, International Institute of Information Technology, Pune, India, 9820794280.

In this paper, the system represents a two server system model where both the servers use symmetric solution of PAKE. Two servers S1 and S2 work simultaneously to authenticate client C also OTP is sent on client's mobile number which finally verifies the client.

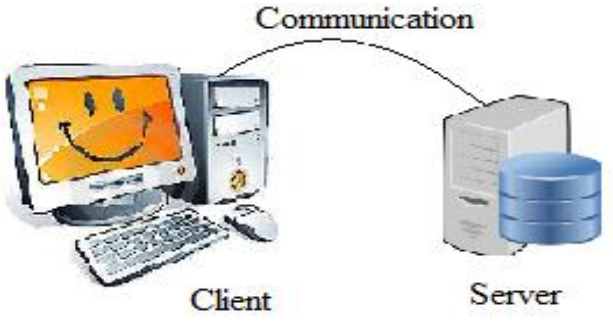

Fig. 1. Single Server System

Client enters password and this password is split into two parts and stored in the servers in an encrypted form. Also in this system even if one of the server gets compromised the attacker still does not get the complete information .No single point failure occurs in this system. This work can further extended with multiple servers.

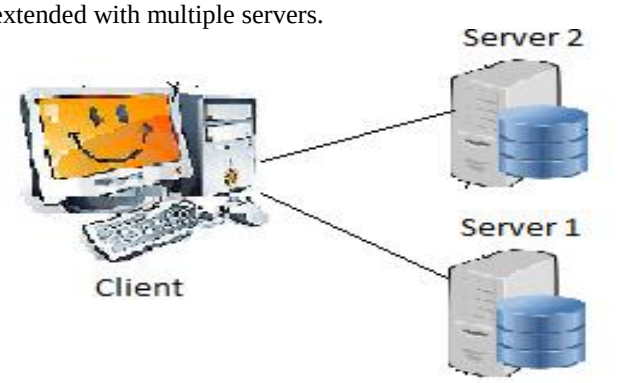

Fig. 2. Two Server System

II. KEY EXCHANGE

Establishing a secure network connection is one of the most important aspect of any message or data transfer protocol. As a secure connection between the active peers is established, the security of the data being transferred increases. To establish such a type of secured and closed connection, the Diffie-Hellman key exchange protocol is used. This protocol originates from the standard hash function (mode-power function) which is used to generate a single secure communication key. This key is used to authenticate communication between client-server and/or server-server for a secure data transfer. This protocol is the first phase of the system where secure connections are established to store passwords into the server and to authenticate the client or user.

Key Exchange

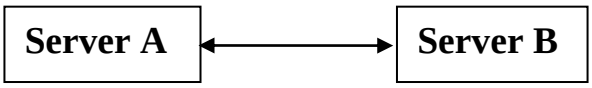

Fig. 3. Key Generation and Exchange

Consider the following scenario. Server A wants to send data 11011 to the server B. Then firstly, server A and server B will communicate with each other and set a secure key (for example *2) for a secure communication. This key, *2, is known to server A and server B only. At the time of data transfer server A will send data 22022 instead of 11011 and server B will receive data 22022. As the server B knows about the key, *2, it will generate original data from data receive by it, i.e., 11011. The above scenario is one using the simplest keys, but to increase the level of abstraction of the system various mathematical computation can be used. The key provides the system with an encoding at the basic level. This is the first frontier which defends the system from attackers.

III. Two Server System

In the previous system only one server was used to store the password. Security provided by this single server is pretty much on the lower side. If the said server gets hacked then the entire information stored in that server is compromised. Also, if the said server is down then the entire system is on a standstill. The users wouldn't be able to authenticate themselves or get access to their information stored on the server. Hence, in order to avoid such situations using two servers is a better solution. It is very difficult for the attacker to know which two servers are used to store the password. Even if the attacker is able to hack into a single server, he will have only half the authentication information. This information is not sufficient to know the password of the user.

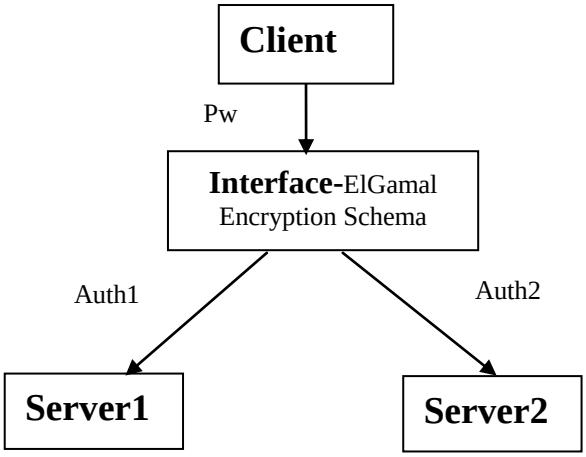

Fig. 4. Generation of Two Authentication Information

The main task of this two server system is to generate two different authentication ids from one password. These two authentication ids then get stored into two different servers. ElGamal encryption is a protocol which generates two cipher texts form single data. Hence, for this two server system ElGamal encryption protocol is used to generate two cipher texts from a single password. Consider the following scenario. Pw is the original password. Cipher texts C1 and C2 are generated with the help of the ElGamal encryption protocol (Figure 4 represents generation of two cipher texts). In figure 4, interface is a machine which is used to connect multiple clients with the server(s).

IV. One Time Password

The system should be more secure. To achieve this we are using One-Time Password (OTP). OTP use a random function to generate secret password. When Client sends a request message to the server, the server generate one time password. Then this password is send on the clients mobile. Client then login using this OTP for authentication. If client do not use this OTP, before timeout period this OTP will vanish. After this timeout for authentication client must again send a request message to the server.

V. Working of System

This system gives the two step verification for the password authentication. First step verification is done by the two server password authentication system and then one time password provide the second level of security. For the first step verification the two server system works in three phases as follows: Initialization, registration and authentication. In this system there are two servers S1 and S2 and a client C. At the first phase server S1 and S2 will communicate with each other and generate a secure key for secure message transfer. To generate the secure key Diffie-Hellman algorithm is required. The key exchange protocol work at this initialization phase. Second phase is user registration phase, when we use any email vendors we have to create an email account there. We are then provided with a user name and password. This phase is called as user registration phase. At this stage, the two authentication ids from the given password are generated with the help of ElGamal protocol. These two authentication ids are then stored in two different servers. At the third phase, the client only remembers password. And for the authentication both the server exchange their information and help to authenticate the client. Whenever next time client login into the system both the servers authenticates client with the help authentication information provided to them. After successful authentication of client, server generate a secret password using a random function. This secret password is the OTP which is sent on the client's mobile number. This OTP is use for client verification. OTP provides additional security to the system.

VI. Conclusion

This system eliminated the risk of passwords being disclosed by introducing two servers. This has overcome the drawback of single server. The system's total running time is equal to running time of single server. Thus, the system is as efficient as a single server in terms of processing time. Our protocol is efficient in terms of computation complexity and communication rounds. We are providing better security by introducing the concept of One-Time-Password in a two-server system. This work can be extended by introducing multiple servers but caution should be taken for the increase in communication rounds, in a multi-server system.

Acknowledgment

We take this opportunity to express our profound gratitude and deep regard to Professor Smita M. Chaudhari, for her exemplary guidance, valuable feedback and constant

encouragement throughout the duration of the project. Her valuable suggestions were of immense help throughout. We also like to thank Professor Sandeep Patil, our respected Head of Department. Working under them was an extremely knowledgeable experience.

REFERENCES

[1] Xun Yi, San Ling, and Huaxiong Wang, "Efficient Two-Server Password-Only Authenticated Key Exchang", IEEE Transactions On Parallel And Distributed Systems, , September 2013.

[2] J. Brainard, A. Jueles, B.S. Kaliski, and M. Szydlo, "A New Two-Server Approach for Authentication with Short Secret," Proc. 12th Conf. USENIX Security Symp., pp. 201-214, 2003.

[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] H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password-Only Two-Server Authenticated Key Exchange System," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.

[5] D. Jablon, "Password Authentication Using Multiple Servers," Proc. Conf. Topics in Cryptology: The Cryptographer's Track at RSA (RSA-CT '01), pp. 344-360, 2001.

[6] Vignesh Kumar K, Angulakshmi T, Manivannan D, Seethalakshmi R and Swaminathan P, "Password Based Two Server Authentication System", Journal of Theoretical and Applied Information Technology May 2012.

[7] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks", Springer-Verlag, 2000.

[8]M. Abdalla, D. Poitcheval, "Simple Password-Based Encrypted Key Exchange Protocols", Proc. CT-RSA, LNCS 3376, pp. 191-208, 2005.

[9] M. Abdalla, M. Bellare, P. Rogaway, "An Encryption Schema Based on TheDiffie-Hellman Problem", 2007.

[10] S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocol Secure against Dictionary Attack," Proc. IEEE Symp. Research in Security and Privacy, pp. 72- 84, 1992.

[11] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. (Crypto '01), pp. 213-229, 2001.

[12] 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.

[13] W. Ford and B.S. Kaliski Jr., "Server-Assisted Generation of a Strong Secret from a Password," Proc. IEEE Ninth Int'l Workshop Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 176-180, 2000.

[14] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586-615, 2003.

[15] D. Jablon, "Password Authentication Using Multiple Servers," Proc. Conf. Topics in Cryptology: The Cryptographer's Track at RSA (RSA-CT '01), pp. 344-360, 2001.

[16] H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password- Only Two-Server Authenticated Key Exchange System," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.

[17] J. Katz, R. Ostrovsky, and M. Yung, "Efficient Password Authenticated Key Exchange Using Human-Memorable Passwords," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (Eurocrypt '01), pp. 457-494, 2001.

Lekha Deshmukh, studying Computer Engineering (batch of 2015) from International Institute of Information Technology- Pune, India. Member of IEEE student's society.

Ankita Kathale, studying Computer Engineering (batch of 2015) from International Institute of Information Technology- Pune, India.

Sayali Kulkarni studying Computer Engineering (batch of 2015) from International Institute of Information Technology- Pune, India.

Prof. Smita M. Chaudhari, Assistant Professor at International Institute of Information Technology- Pune, India. Pursued B.E. in Computer Engineering in 1999. Pursued M.E. in Computer Engineering in 2011. Expertise in System Security, Computer Networks, Database Management Systems.