IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Two Server Authentication using Shared Key Cryptography

Arati Sonawane[1], Ashwini Patil[2], Kuntal Bhangale[3]

UG Students, Department of Computer Engineering, SSBT's College of Engineering and Technology, North Maharashtra University, Jalgaon, Maharashtra, India[1,2,3]

Abstract: For many years peoples were used to send the message using the post office and other media which is not that secure. Passwords are commonly used by people during log in process to access such as computer, ATM, network, etc. Earlier password based authentication strategy are used with assume single server stored all password to authenticate the client during authentication. In earlier system the passwords necessary which is stored in a single server while authenticate client. The attacker can easily hack on single server, contain all data regarding password are easily available to attacker. In proposed system, where a client and a server, who share a password to authenticate each other and meanwhile establish a cryptographic key by share of messages. Propose system two server authentications, where a password is split into two parts, which are securely share on to the two servers during authentication using the PAKE protocol. The Protocol runs in parallel and is more efficient than existing.

Keywords: Security, shared key, password authentication, public key authentication.

I. INTRODUCTION

For that uses the password. Passwords are commonly used by people during log in process to access such as computer, ATM, network, etc. Earlier password based authentication strategy are used with assume single server stored all password to authenticate the client during authentication. The project aims at making an efficient password Authentication protocol. An efficient password based authentication allowed to establish secure cryptography key for secure communication after authentication. A Diffie-Hellman key exchange which is use to establish shared key over unprotected communication channel and ElGamal encryption scheme will be implement for key generation, encryption and decryption. The password based authentication will be developed with help of PKI and Password-only modes.

Motivation

To make an efficient password based authentication protocol. The password authentication is introduced with Diffie-Hellman and ElGamal algorithm and to make the secure communication, in PKI model the client can send the password to the server by public key encryption and password only model is used as secret key for key exchange purpose. Which is beneficial when the one server is hack by the attacker, the attacker still cannot be retrieving the information from that server.

II. LITERATURE SURVEY

The content of the paper focuses on the research and contributions of various sources. These include:

[1] The paper describes the basic uses of the password and the basic secret sharing scheme. The secure communication after authentication and secret sharing are discussed in detail. The existing secret system faces a drawback of retrieve of secret, even the without a valid share. The paper proposed the concept of the sense that two peer servers equally contribute to the authentication. In this way valid secret sharing possible.

[2] The paper describes the role of public key infrastructure technique in detail. The paper describes the paper key of registered users. The various cryptography encryption algorithms are also described in paper. The concept of secret sharing communication and uses of public key infrastructure technique is also discussed in detail.

[3] The paper describes the authentication protocol. The paper describes the security based authentication protocol that is associated with and without key exchange. In the paper two-party authentication protocols providing authenticated key exchange, which focuses on those using asymmetric techniques. A simple, efficient protocol referred to as the station-to-station protocol is introduced.

Table1: Literature Survey

Authors	Description	Limitation
Xun Yi, San Ling, and Huaxiong Wang.	The paper describes the basic uses of the password and the basic secret sharing scheme. The secure communication after authentication and secret sharing are discussed in detail.The paper proposed the concept of the sense that two peer servers equally contribute to the authentication.	The paper describes only password only authentication model for secure communication. Paper represent a symmeteic solution for two server authentication protocol.
Jae Hyung Koo, Bum Han Kim, and Dong Hoon Lee.	The paper describes the role of public key infrastructure technique in detail. The paper describes the paper key of registered users. The various cryptography encryption algorithm are also described in paper. The concept of secret sharing communication and uses of public key infrastructure technique is also discussed in detail.	The paper shows only public key infrastructure.This paper represent certificate authority for validate the certificate.
Whitfield Diffie, Paul C. van Oorschot and Michael J. Wiener.	In the paper two-party authentication protocols providing authenticated key exchange, which focuses on those using asymmetric techniques. A simple,efficient protocol referred to as the station-to-station protocol is introduced.	The paper involves only asymmetric authentication protocol.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

III. PROPOSED SYSTEM

The proposed system is a solution in authentication using password-based allowed a client and servers meanwhile to authenticate with a password and establish a secure cryptographic key for secure communications after authentication. In proposed solutions for password based authentication models.

Problem Definition
Secure social network is a necessity in today's life. Among various mechanism is use to secure a transmission on the network. Secure a password, the concept of two way security mechanism is use in which password is divided on two server. The elgamal encryption Algorithm is used to store a password on two server. With the presence of one server, the user is not able to login the system. Because of this only authenticated user login the system.

• Diffie-Hellman Algorithm
This algorithm use for sharing a password over an unprotected communication network.

• Elgamal Algorithm
Elgamal algorithm use for key generation, encryption, decryption. Encryption algorithm will encrypt password and divide password on two server to provide more security to user

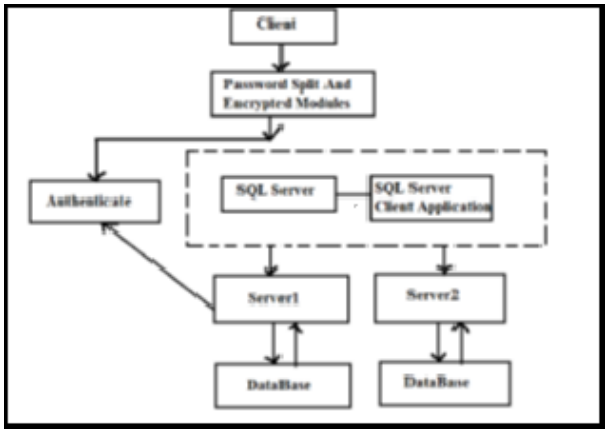

Fig1: Proposed System Architecture

• Registration:
At the time of registration, the password and other information entered, where a password is split into two parts, which are securely distributed on to the two servers, during registration. Although we refer to the concept of public key system, the encryption key of one server of values should be unknown to second server and the client needs to remember a password after registration.
• Login:
When the user login for an system, enters the asked details in the form including the username and the password. The entered password has to be in character in length. The constraints for the username include that each user must have a unique email id. So a username once registered cannot be used again by another user. Once the details are submitted, the password is sent to the next module (next module) to start the encryption process.
• Split Password and encryption
When login has sucessfully done. Then the password was split into two servers that are server1 and server2 (for example, 'abcd' store in server1 and '1234' is stored in server2). The authentication algorithm i.e. Eglamal algorithm is apply this store in the servers.

IV. IMPLEMENTATION

Implementation involves the environment in which system is implemented and overall system development. Overall system development requires suitable environment and proper resources for successful completion. Proposed system is developing for secure communication between client and server. At the server the password is divided into two servers that is server1 and server2. At a time of authentication is takes place password is extracted from both the server and authenticate.

Flow of system development
Flow of system development consists of sequence of implementation by which the system or software is implemented.

Step 1: Users Register to System by giving user name and a password.
Step 2: User Information will then be split into two parts on two different servers server1 and server2.
Step 3:ElGamal Encryption process has been applied to store the password into two servers.
Step 4: The information has then be stored into the two servers with password split into two parts.
Step 5: The user logs in with the original credential.
Step 6: The user password will again split into two parts.
Step 7: elGamal process is applied to decrypt the passwords from two servers.
Step 8: If password from two servers matches then report successful login.
Step 9: If password from two servers doesnt match then report error.

V. RESULTS

• Results and Analysis for Server
At the server side, the password in the form of number, string, special characters, or a combination of these is converted into encrypted form.

Table2: Result for Server

Server 1	Enter Password : y12345 Server Key 1 : y12 Server Key After Encryption : 121049050 ConString :jdbc:mysql://localhost:3306/serv1 Established Connection With Server 1 Registered Successfully With Server 1.
Server 2	 Server Key 2 : 345 Server Key After Encryption : 051052053 Established Connection With Server 2 Registered Successfully With Server 2

DOI 10.17148/IJARCCE.2016.54166

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

The password is then split into two servers which is in the form of encrypted password. While the authentication is takes place it check the password which is situated on two servers. If the password is valid then authentication takes place and login successfully otherwise not. Table2 shows the results of the servers of the proposed system.

• Result and Analysis for client

At the Client side, the encrypted string is received from the server. First client done

registration after registration password is store on two servers. At a time of login client needs correct password, extract password from servers which receive at a time of registration. Client also have facility of change password. At client side Table3 shows registration, login process shows in Table4, Table5 shows change password and result for exit is shown in Table6.

Table3: Result for Registration for client

Registration	Enter Name of User : yogi Enter Location of User : jalgaon Enter Email Address (to be used in login) : y@gmail.com Enter Password : y12345 Server Key 1 : y12 Server Key After Encryption : 121049050 ConString :jdbc:mysql://localhost:3306/serv1 Established Connection With Server 1 Registered Successfully With Server 1 Server Key 2 : 345 Server Key After Encryption : 051052053 Established Connection With Server 2 Registered Successfully With Server 2.

Table4: Result for Login process for client

Login	Enter Email Address : y@gmail.com Enter Password : y12345 Server Key 1 : y12 Server Key After Encryption : 121049050 Server Key 1 : 345 Server Key After Encryption : 051052053 Server 1 : 121049050 , 121049050 Server 2 : 051052053 , 051052053 Login Successful. --- Enter Email Address : y@gmail.com Enter Password : 1234yg Server Key 1 : 123 Server Key After Encryption : 049050051 Server Key 1 : 4yg Server Key After Encryption : 052121103 Server 1 : 049050051 , 121049050 Server 2 : 052121103 , 051052053 Invalid Username or Password s1

Table5: Result for change password for client

Change Password	Enter Email Address : y@gmail.com Enter Password : y12345 Enter New Passwordy123 Server Key 1 : y12 Server Key After Encryption : 121049050 Server Key 1 : 345 Server Key After Encryption : 051052053 Server 1 : 121049050 , 121049050 Server 2 : 051052053 , 051052053 Server Key 1 : y1 Server Key After Encryption : 121049 ConString :jdbc:mysql://localhost:3306/serv1 Established Connection With Server 1 Update Password Successfully With Server 1 Server Key 1 : 23 Server Key After Encryption : 050051 ConString :jdbc:mysql://localhost:3306/serv2 Established Connection With Server 2 Update Password Successfully With Server 2

Table6: Result for exit from client

Exit	Bye Bye ..... !

VI. CONCLUSION

In the paper presented a symmetric protocol for two-server password-only authentication and key exchange. The protocol is securing both against passive and active attacks in case that one of the two servers is compromised. Regarding Performance protocol is more efficient and secure than existing symmetric and asymmetric protocol two-server password Authentication Shared Key protocol.

REFERENCES

[1] Xun Yi, San Ling, and Huaxiong Wang, "Efficient Two-Server Password-Only Authenticated Key Exchange", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, pp. 1045-9219, SEPTEMBER 2013. (Research Paper)

[2] Jae Hyung Koo, Bum Han Kim, and Dong Hoon Lee "Authenticated Public Key Distribution Scheme Without Trusted Third Party", CIST, korea university, Seoul, Korea, pp. 926-935, 2005. (Research Paper)

[3] Whitfield Diffie, Paul C. van Oorschot and Michael J. Wiener "Authentication and Authenticated Key Exchanges ", Bell-Northern Research, P.O. Box 3511 Station C, Ottawa, Ontario K1Y 4H7 Canada, pp. 107-125, 1992. (Research Paper)

[4] H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password-Only Two-Server Authenticated Key Exchange System", Proc. Ninth Intl Conf. Information and Comm. Security (ICICS07), pp. 44-56, 2007. (Research Paper)

[5] M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.

[6] M. Abdalla, O. Chevassut, and D. Pointcheval, "One-Time Verifier-Based Encrypted Key Exchange," Proc. Eighth Int'l Conf. Theory and Practice in Public Key Cryptography (PKC '05), pp. 47-64, 2005.