Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.216 – 221

RESEARCH ARTICLE

Improving Service Credibility in Password Authentication Peer Service

S. Bhuvanesh[1], L. Anita Elizabeth[2]

[1] Department of IT, Sri Venkateswara College Of Engineering, India

[2] Department of IT, Sri Venkateswara College Of Engineering, India

[1] bhuvaneshjayam1988@gmail.com; [2] lanita@svce.ac.in

Abstract— ***Two server password-based authentication protocols (Two-Server PAKE), where two servers co-operate to authenticate a client on the basis of Password only and if one server is compromised due to Insider Attack or Distributed Denial Of Service Attack (DDOS). In Asymmetric two-server PAKE protocol runs in series and only the front-end server and the client need to establish a secret session key. In Two-Server PAKE protocol has been symmetric is not efficient for practical use. So, a Symmetric Two-Server PAKE protocol which supports two servers to compute in parallel to authenticate a client by Encrypted key exchange(EKE) and meanwhile keeps efficiency for practical use. It requires only four communication rounds for the client and two servers mutually to authenticate and simultaneously to establish secret session keys.***

Keywords— ***PAKE; Symmetric; Asymmetric; EKE***

I. INTRODUCTION

Ordinary people seem to have a fundamental inability to remember anything larger than a small secret. Yet most methods of remote secret-based authentication presume the secret to be large. We really want to use an easily memorized small secret password, and not to be vulnerable to dictionary attack. In this paper, we make a clear distinction between passwords and keys: Passwords must be memorized, and can be recorded easily. Most methods need keys that are too large to be easily remembered is the problem faced. User-selected passwords are often cramped to a very small and to increase the size of the space just make them hard to remember. Bank-card PIN codes use only 4-digits (about 13 bits) to remove even the temptation to write them down. A ten-digit phone number has about 30 bits, which compels many people to record them. In most cases, strong symmetric keys need 60 bits or more, and nobody talks about public-keys which can be memorized. Assume that a memorisable password belongs to a brute-force searchable space. There is a growing gap between the size of the smallest safe key and the size of the largest easily remembered password with increasing power.

Unfortunately most commonly known remote password methods required large password. To counter the attack, user assigns the passwords large, we force frequent password changes, and we issue guilt-instilling mandates to never write the password down. It's almost as if there's an unspoken, cavalier attitude toward the users problem: "They can't remember a very large enough password, and then they will get justify." Users themselves to protect and avoid password memorizing method. Our system is a password-only system in the sense that it requires no public key and thus, no PKI. This system very attractive considering PKIs is proven notoriously expensive to deploy in the world. Moreover, a proposed system is particularly suitable for resource constrained users due to its efficiency in terms of both computation and communication. We generalize the basic two-server model to architecture of a single back-end server supporting multiple front-end servers and envision interesting applications in federated enterprises.

II. **ANALYSIS AND ARCHITECTURE**

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

A. ANALYSIS

Most of the existing password systems were designed over a single server, some password verification data with a single authentication server. Systems are essentially deliberate to defeat offline dictionary attacks by outside attackers and assume that the user password is completely trusted in protecting the database and sever. The attackers in practice take on a variety of forms, such as , accidents, disgruntled system administrators and misconfigurations. As a result, no security measures and precautions can guarantee that a system will never be penetrated. Once an authentication server is accord by all the user passwords or in the hands of the attackers of PVD fall, who are definitely effective in offline dictionary attacks against the user passwords.

Two server password-based authentication protocols (Two-Server PAKE), where two servers co-operate to authenticate a client on the basis of Password Only and if one server is compromised due to Insider Attack or Denial Of Service Attack (DDOS), the attacker still cannot pretend to be the client with the information from the accord server. Recent research about password-based authentication and follow two models. The first model, called public key infrastructure(PKI)-based model, assumes the client keeps the server's public key in addition to share a password with the server. The client can send the password to the server by public key encryption. The second model is called password-only model which follows encrypted key exchange (EKE) protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose. A password-only authentication protocol which is both practical and provably-secure under standard cryptographic assumption. Our Protocol is Symmetric and, can run in parallel to establishes secret session keys between the client and two servers. One of the two servers shuts down due to the denial-of service attack, by using another server can continue to provide services to trusted clients. In the parallel computation and reliable service, a symmetric protocol is very much useful compare to an asymmetric protocol.

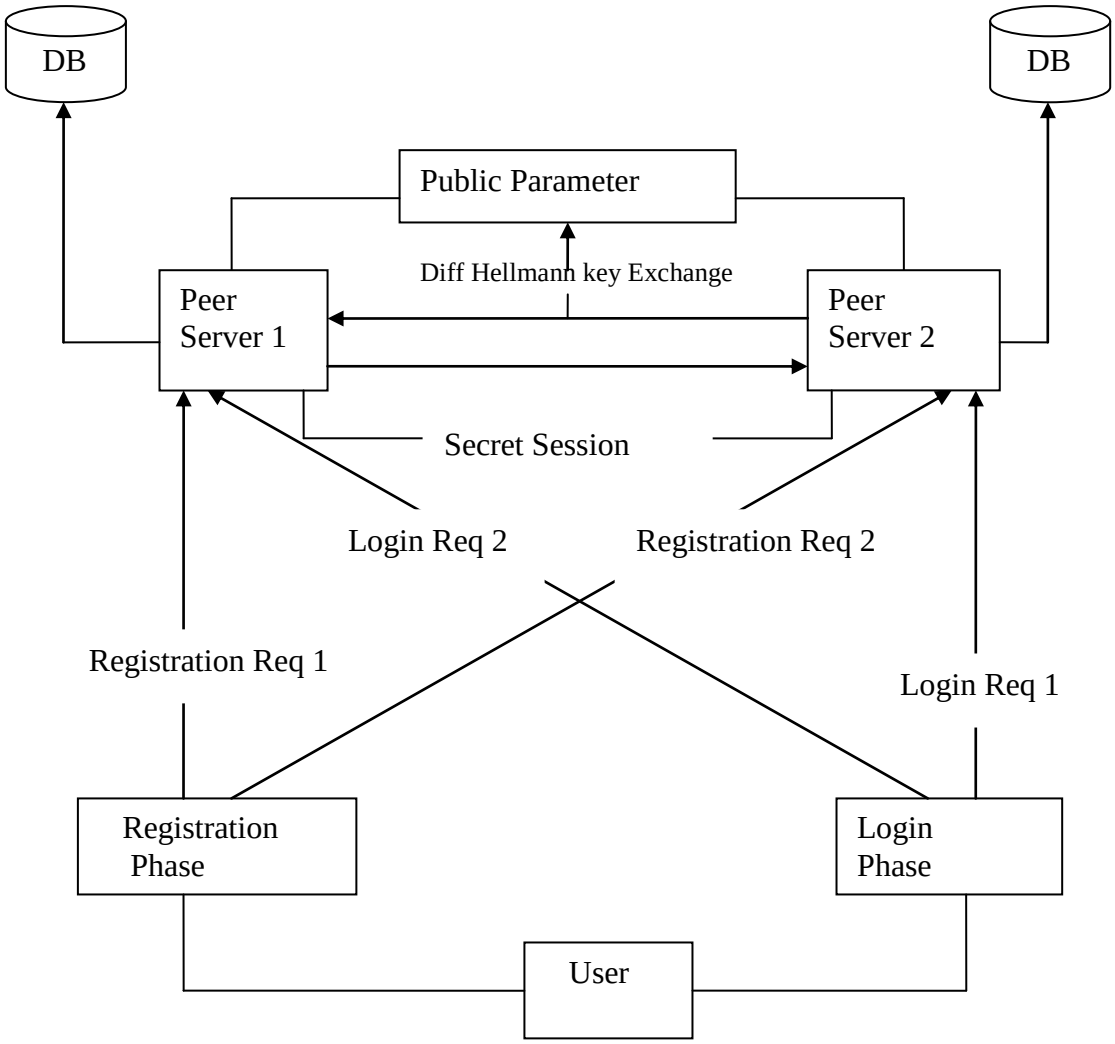

FIGURE 1: INTIALIZATION

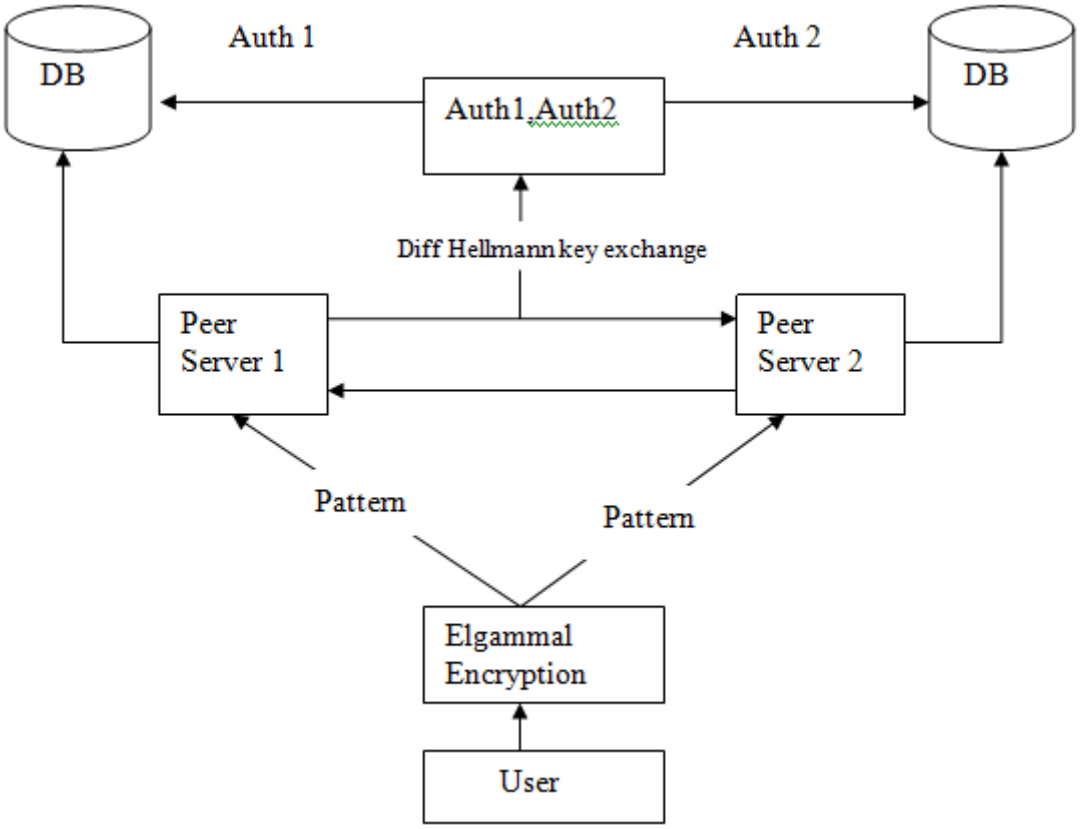

FIGURE 2:REGISTRATION AND AUTHENTICATION

B. REQUIREMENT

1.Software Requirements

FORNT END:Java 1.4

BACK END :Sql/Tomcat

2.Hardware Requirements

PROCESSOR:Core i3

HARD DISK :20gb

RAM :128mb

OPERATING SYSTEM:Windows 7

III. DEVELOPMENT AND MODULES

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

A. SYSTEM INITIALIZATION

The two peer servers S1 and S2 jointly choose a cyclic group G of large prime order q with a generator g1 .Next, S1 randomly chooses an integer s1 from Z* q and S2 randomly chooses an integer s2 from Z * q , and S1 and S2 exchange g1^s1 and g1^s2 . After that, S1 and S2 jointly publish public system parameters G, q, g1, g2 , where g2 = g^s1s2 .

B. SECERT KEY ESTABLISHMENT

The J2EE Environment is setup and Two Peer Servers are initialized and release the public parameters for the user by exchange of keys using Diffie-Helman key Exchange. Two Servers for further secure communication for Peer Servers for that Secret key is established. The Secret Session will ensure that the two servers are Genuinely involved in the process of User Registration and Authentication to provide Peer Services for the Genuine User. Our protocol runs in three phases Of Which Initialization comes Under Secret Key Establishment which uses Diffie-Helman key Exchange.

C. REGISTRATION AND AUTHENTICATION

We refer to the concept of public key, the encryption key of one server should be unknown to another server and the client needs to remember a password only after registration. Each client C is required to register both S1 and S2 through different secure channels. The client C generates decryption and encryption key pairs (xi, yi) where yi = g1^xi 1 for the server Si (i = 1, 2) using the public parameters published by the two peer servers. The client C chooses a password pwC and encrypts the password using the encryption key y, according to ElGamal encryption. At last, the client C delivers the password authentication information Auth(1) C = {x1, a1, b1, E(g2^pwC , y2)} to S1 through a channel, and the password authentication information are secured through Auth(2) C = {x2, a2, b2, E(g2^pwC , y1)} to S2 through another secure channel. The client C remembers the password pwC after that only.

The two servers S1 and S2 have received the password authentication information of a client C based on authenticstion. The following steps are involved in the process of Authentication.

1. The client C randomly chooses an integer r from Z * q , computes R = g1 ^ r * g 2 ^ −pwC and then broadcasts a request message M1 = {C,Req,R} to the two servers S1 and S2
2. The Diffe-Helman Key Exchange Occurs between Peer Servers Which run in parallel and establishes a secret session to fetch the password authentication Information and the two servers mutually generate two values

to send Hash functions to Client based on their Password Authentication Information.

3. The client computes the Hash functions sent and Ex-or ing the Hashes will produce the Hash of his own Password. If the Password Hash and computed Hash are same the cli8ent can ensure that he is connected with Genuine Servers and can continue enjoying Services from Peer Servers without worry.
4. So the user needs to remember the Password Only authentication. He is safe and secure under our Proposed Model.

IV. **IMPLEMENTATION**

A password authentication and key exchange protocols upon the two server model is presented in this project. It's a two-server password system in which one server exposes it to users and the other is hidden from the public. This two server model appears to be a sound model for practical applications. This approach is based on Key-Exchange system because the public created for the user and the service server is shared between them. In such architecture, the control server and the service servers are managed in different administrative domains, and the domain where the control server resides enforces more stringent security measurements.

V. **CONCLUSIONS**

A password-based authentication and key exchange system is proposed that is built upon a novel two-server model, where only one server communicates to users while the other server stays transparent to the public. Compared with existing solutions, this system possesses many advantages, such as the elimination of a single point of, avoidance of PKI, and high efficiency. In contrast to multi-server password systems, the proposed system has great potential for practical use. It can be applied to fortify existing standard single server password applications directly, web applications. It can also be applied in the single control server supports multiple service servers.

REFERENCES

[1] X. Yi, R. Tso, and E. Okamoto, "Identity-Based Password Authenticated Key Exchange for Client/Server Model," Proc. Int'l Conf. Security and Cryptography (SECRYPT '12),pp. 45-54, 2012.

[2] X. Yi, R. Tso, and E. Okamoto, "Three-Party Password-Authenticated Key Exchange without Random Oracles," Proc. Int'l Conf. Security and Cryptography (SECRYPT '11),pp. 15-24, 2011.

[3] 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.

[4] Y. Yang, R.H. Deng, and F. Bao, "Fortifying Password Authentication in Integrated Healthcare Delivery Systems," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), pp. 255-265, 2006.

[5] 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.

[6] Y. Yang, R.H. Deng, and F. Bao, "A Practical Password-Based Two-Server Authentication and key Exchange System," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 2, pp. 105-114, Apr.-June 2006.

[7] Y. Yang, F. Bao, and R.H. Deng, "A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprise," Proc. 20th IFIP Int'l Information Security Conf. (SEC'05), pp. 95-111, 2005.

[8] M. Szydlo and B. Kaliski, "Proofs for Two-Server Password Authentication," Proc. Int'l Conf. Topics in Cryptology (RSA-CT '05), pp. 227-244, 2005.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] M. Di Raimondo and R. Gennaro, "Provably Secure Threshold Password Authenticated Key Exchange," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt '03),pp.507-523,2003.

