International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

To Secure Efficient Two-Server Password and Authenticate Key Exchange using Transaction Processing System against Dictionary Attack

Sonal Chandrakant Pansare[1], V. S. Nandedkar[2]

[1]II[nd] Year ME, Department of Computer Engineering, PVPIT, SavitribaiPhule Pune University, Pune , India

[2]Associate Professor , Department of Computer Engineering, PVPIT, SavitribaiPhule Pune University, Pune , India

Abstract: ***A user and a server, who exchange their data or messages by using cryptographic key as well as sharing the password and authenticate with each other, this is the primary approach for password-Authenticated Key Exchange (PAKE). In the existing work, there are dualistic solutions for two-server PAKE either symmetric or asymmetric. In this it presents asymmetric solution for two-server PAKE, where a user can create various cryptographic solutions to the two servers. The current asymmetric two-server PAKE protocols are used in parallel computation. The proposed work extends the model by imposing different levels of trust upon the two servers, and generates a unique method at the technical level in the designing of protocol. As a result, we propose a practical two-server password authentication and key exchange system that is secure against offline dictionary attacks by servers when they are controlled by adversaries. Our proposed scheme is, a password-only system in the sense that it requires no public key cryptosystem and, no PKI. In the proposed system it introduced the new technique which is TTP (i.e., Trusted Third Party) server where, a user's data will be passed on to the TTP server via web-service access in SOAP protocol by using the TPS i.e., Transaction Processing System and then the true encrypted data will send it to both the servers. The paper work, generalize the single back-end server architecture for basic two server model to supports the multiple front-end servers and for the federated enterprises of envision interesting applications. In the authentication system , to provide the more security we use SMS integration API for two step verification like Gmail.***

Keywords: Password-authenticated key exchange (PAKE), Diffie-Hellmen key exchange, ElGamal encryption, SOAP, TPS, Two-Step Verification.

1. Introduction

In a recent days, peoples are commonly used a passwords by their process of login to controls the operating systems, mobile phones, television, automated teller machines and so on. Passwords are requires for many purposes to accessing a computer user. In a period of, a cryptographic hash function is transmitted the password over a public channel that an attacker can access a hash value; this is done in password-based authentication systems. In the existing work, there is dualistic solution for two-server PAKE either symmetric or symmetric. In symmetric, for the authentication that contributes the equal work to two-peer servers and in asymmetric, where user can create various cryptographic solutions for the two-servers [1]. Also their result shows in series that the user need to generate a secret session key (password). Despite the fact that we use the idea of public key cryptosystem but our protocol said to use the password only model. In this model we use for two servers of the set of two things is an encryption and decryption keys [2]. In encryption two servers, generated the secure session keys to the user and the servers via distinct secure medium. Whereas in decryption two-server PAKE protocol works as a user that divide equally between two which sends secret password to two-servers. In this, we use the two algorithms for two-server protocols is; Diffie-Hellman key exchange and ElGamal ecryption scheme [8], [9], [11], [13]. A dictionary attack is a method of breaking into a password protected computer or server by systematically as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message. A dictionary attack is primarily used against password. Encryption algorithms are seldom attacked with a dictionary attack because most times they use a random number as key. A typical dictionary for this attack would contain the most used passwords.

2. Background

2.1 Multiple-Server Password Model [3]

In multiple-server password model as Figure 1 shows, at the server side having multiple servers that to eliminates the results involves in the single server model which in terms of offline dictionary attacks for single point of vulnerability in opposition to the user password database. The multiple servers make a settlement in the way of eliminating the single point of vulnerability, that the servers are disclosure to having the same for the users and a user has to transmit in parallel with all servers for authentication. But the problem with this model is a firm on imparting information bandwidth and the demand for semaphores at the user side from the time that a same user has to engage in occurring at the same time of sharing with multiple servers. In the security point of view servers are equally disclosure to outside attackers.

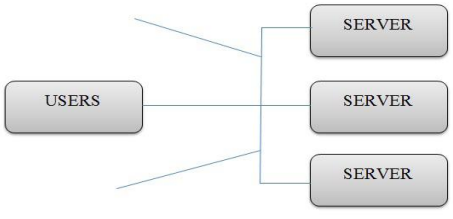


Figure 1: Multiple-Server Password Model

2.2 Increase of Gateway in Multiple-Server Model / Multiple-Server Model with increase of Gateway [3],[15]

As shown in Figure 2, a Gateway is re-transmitting device between users and servers. Performance of the Gateway is to remove or eliminates the sharing with multiple servers multiple-server model. So for this, the Gateway inserts an extra layer in the model, which performs a superfluous since for the users and the servers and the Gateway device where it performs the re-transmitting between users and servers, also it does not in any such way that engage within the authentication, security performance, services to the process of providing things.

Figure 2: Gateway in Multiple-Server Password Model

2.3 Two-Server Model [3],[15]

In Figure 3 shows that, in two-server model there consist of two servers at the server side, in that case there are two ways to place the server. One way to access which is a public server that disclosure reflexive from of it to users i.e., front-end server and other way to access which is back-end or private server in the place where to the rear of occurs.

Figure 3: Two-Server Model

A user which is finishes with to make permanent or secure a secret key accompanied by the public server i.e., front-end and the performance of the back-end server i.e., private server in user authentication which is no more as a subordinate to the public server [1], [8]. For security point of view,is nothing besides from a public server which is an aspect of about to the server side security and taking the all aspects into the two-server model. The back-end server is more trustworthy than a public server. Since the front-end server is a public server which is more likely attacked from the attacker i.e., not secure against the attacker; logically the back-end server is hidden from the public which is not attacked i.e., secure against the attacker.

3. Literature Survey

3.1 Existing System

In, Katz et al [8] proposed a symmetric two-server PAKE protocol, their extended protocol is Katz-Ostrovsky-Yang PAKE i.e., KOY protocol; in this two-server runs from going continuously at the same distance from each other and make permanent or secure in the space of user and two servers with secret session keys. But their protocols are no more used in practical point of view for their inefficiency.

In, Brainard et.al.s [10] establish gradually which work in Yang et al imply an asymmetric setting, which is having two servers i.e., front-end and back-end server; where font-end server interacts with the user, while a back-end server helps to the front-end server with authentication. Yang et al put forwards for consideration of a PKI-based asymmetric two-server PAKE protocol.

Also, Yang et al [9], [12] proposed a few asymmetric password only two-server PAKE protocols, in this a front-end server admit to begin for a request. In this their protocols having more efficiency for practical use than the Katz et al protocols. But their protocol requires two servers for computations of the servers or communication round that are more and also runs in series.

In, Jin [11] improved the performance of Yang et al's protocol which is their communication rounds may require less than the Yang et al's protocol; for that Jin proposed a new symmetric two-server PAKE protocol. In their protocol the user sends the hash value i.e., H to all the users with the front-end as well as back-end server. But in their protocol structure which need to runs in a series of the two servers.

In, Wei-Kno Chiang [14] is suggested two –server PAKE protocols which is an efficient for protecting the in secure network within the communication to sharing a secret session key. Their protocol proposed a key exchange protocol using Diffie-Hellman which appearing a secret session key without enables the exchange protocol in the message. In this paper, we proposed a two servers. This two servers cooperate and provide services to authenticated users. A user chooses password and cannot authenticate unless both the servers collude. The two servers cooperate to authenticate the user. In our protocol, the user and the two servers communicate through a public channel; while the back-end server is a control server whose sole purpose is to assist the service server i.e., front-end server in user authentication.

A. Drawbacks of Existing System

- Key Management Issues
- If Server Rounds are more then, the Computation Time is also more
- Data Integrity
- Data Inconsistency

4. Proposed System: Pakets Architecture

System architecture shown in Figure 4, is the view of conceptual model which is defined the behavior, structural and many views of the system. A formal description and representation of the system architecture to organized in a way that supports reasoning about the structures of the system. PAKE i.e., Password Authenticate Key Exchange is where a user and a servers, who share a password, authenticate each other and meanwhile establish a cryptographic key by exchange of message. In a user side they will be two algorithms applied i.e., Diffie-Hellmen key exchange and ElGamal encryption by working in three phases which is, first phase having initializing and registration, second phase is web-service access in SOAP protocol which works in TPS i.e., Transaction Processing System, and third phase is login phase i.e., authenticate the key. So the data will be passed on to TTP (Trusted Third Party) server web service access in SOAP protocol. TTP

server acts as a router that transmits the data to both the database servers i.e., database server 1 and database server 2; TTP server does not validate to the authenticated of data received. The database server 1 and 2 will only store the encryption data. If any false data is encountered then these servers will send back the data to TTP server, and the TTP server will send the same data back to the user's login phase for correction of data and then same procedure will be taken place at the start.

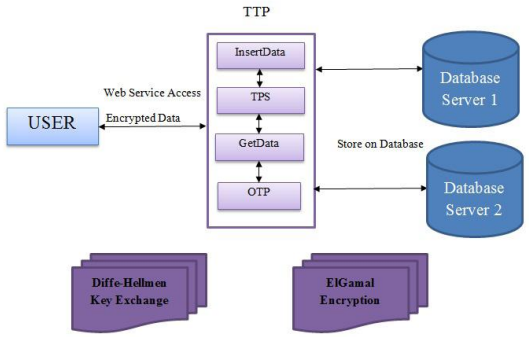
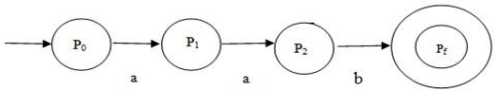


Figure 4.PAKETS System Architecture

A. Mathematical Model for PAKETS



States :

DFA= {Q, ∑, δ, q_0, F}, Where

Q=Finite Set of States, ∑=Input Alphabet, δ=Transition between states, P_0=Initial State, P_f=Final State, Q= {P_0, P_1, P_2, P_f}.

Operations:

P_0=Initial State

P_1=Key initialization

P_2=encryption

P_3=OTP verification

P_f=decryption

∑= {a, b} Where,

a= is the input query parameter given by user

b=output of particular query (resultset)

5. Algorithms

5.1 Diffie-Hellman Key Exchange Protocol

Diffie-Hellman set up the shared secret key for exchanging data excessively in a public network [8], [9] where they can be access secret communication. Diffie-Hellman key exchange protocol which appears a secret session key without enables the key exchange protocol in the message or communication. The implementation of Diffie-Hellman which is introduce [11] two users Alice and Bob, whereas they communicating excessively a medium with felt to approve of an two positive numbers p and g, where p is a prime number and g is a generator of p. Once Alice and Bob have approved of on p and g in private, they select a random number u and v respectively.

Algorithm of Diffie-Hellman Key Exchange	
Input: Shared Secret Key for Exchanging Data	
Step1	$A = g^u \bmod p$
Step 2	$B = g^v \bmod p$
Step 3	The two users share their public keys A and B over a communication medium such as the Internet.
Step 4	$K_1 = B^u \bmod q$
Step 5	Bob computes K2 using, $K_2 = B^v \bmod q$ Where, K_1 and K_2 is a shared secret key using the two users Alice and Bob.
Output: Key Exchanged	

5.2 ElGamal Encryption scheme

The ElGamal encryption system is an asymmetric key encryption algorithm used in cryptography [13] where public key cryptography. The Diffie-Hellman key exchange protocol where supported for the encryption system. It includes key generation, encryption and decryption algorithms.

- **Key Generation**

Algorithm of ElGamal Encryption scheme	
Input: ElGamal Key Generation	
Step 1	Alice generates multiplicative cycle group G of order p with generator g.
Step 2	Alice selects a random number x from 1,. . . , (p-1).
Step 3	The two users share their public keys A and B over a communication medium such as the Internet.
Step 4	Alice computes h = gx
Step 5	Alice introduces h for their public key i.e., (G, g, p, h).
Output: Key Generated	

- **Encryption**

The following is the encryption algorithm to encrypt a message m to Alice under her public key (G, g, p, h).

Algorithm of ElGamal Encryption scheme	
Input: ElGamal Encryption	
Step 1	Bob selects a random number y from 1, . . . , (p-1); then calculate c1 = gy.
Step 2	Bob calculates the shared secret key s = hy .
Step 3	Bob converts his secret message into an element m and G.
Step 4	Bob calculates c2 = (m*s)
Step 5	Bob sends the cipher text $(c1; c2) = (g^y; m; (g^x)^y)$ to Alice.
Output: Key Encrypted	

- **Decryption :**

The following is the decryption algorithm to decrypt a cipher text (c1, c2) with her private key x;

Algorithm of ElGamal Encryption scheme	
Input: ElGamal Decryption	
Step1	Alice calculates the shared secret $s = c_1^x c_1^x$.
Step 2	And then computes m '= c2 . s-1 which she then converts back into the plaintext message m, where s-1 inverse of sin the group G.
Step 3	The decryption algorithm produces the intended message, Since $c_2.s^{-1} = m^1.h^y.g^{xy-1} = m^1.g^{xy}.g^{-xy} = m^1$
Output: Key Decrypted	

5.3 TPS (Transaction Processing System)

Transaction processing system algorithm is use for removing the data inconsistency problem. A system failure is modelled by assuming that the state of the system in the volatile memory is lost, but the state in the non-volatile memory survives following the system failure. The recovery from system failure involves the following:

(a) The effects of transactions that were in committed state at the time of the system failure must be incorporated into the data.
(b) The effects of transactions that were aborted or were active at the time of the system failure must be eliminated.
Note that transactions that were active when the failure occurs are considered aborted since their internal state is lost due to the failure.

5.4 Two-Step Verification

Algorithm of Two-Step Verification	
Input: Mobile User Verification	

Step1	A seed (starting value) s is chosen.
	S →S0 ; // Initialize the state.
	for k in 1, 2, ..., m do // Scan the input data units:
	S →F(S, b[k]) // Combine data unit k into the state.
	return G(S, n) // Extract the hash value from the state

Step 2	A hash function f(s) is applied repeatedly (for example,1000 times) to the seed, giving a value of: f(f(f(.... f(s) ....))). This value, which we will call f^{1000} (s) is stored on the target system. N It can be shown that if f is a pseudo-random number generator for the uniform distribution on (0,1) and if is the CDF of some given probability distribution , where F*:(0,1) →R is the percentile of P Intuitively, an arbitrary distribution can be simulated from a simulation of the standard uniform distribution.
Output: Verification Successfully	

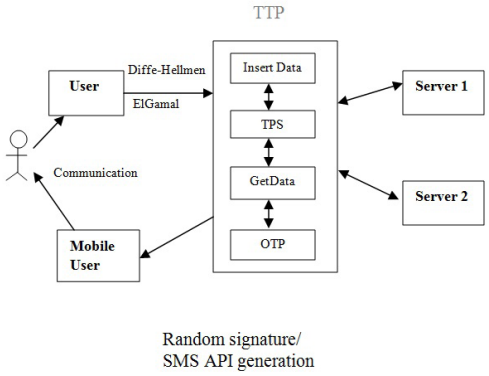


Figure 5: Two-Step Verification

6. Results

Figure 6.a.shows data encryption performance which works to show that the data it will encrypt in how much time in seconds. Suppose there is a 100kb data is encrypted in 150 sec so the result will display automatically in that time of encryption data from the users. In Figure 6.b.shows the existing system and proposed system performance, which is the server rounds performance. In this result graph shows the no. of server rounds, in the existing system total no. of server rounds is 7(seven) to send the users true data to database servers that means this system is complex to handle and also having data loss or stolen, whereas in proposed system there is only 3(three) server rounds that sends the users true or private data to database servers without having any loss and the system will secure from any other systems.

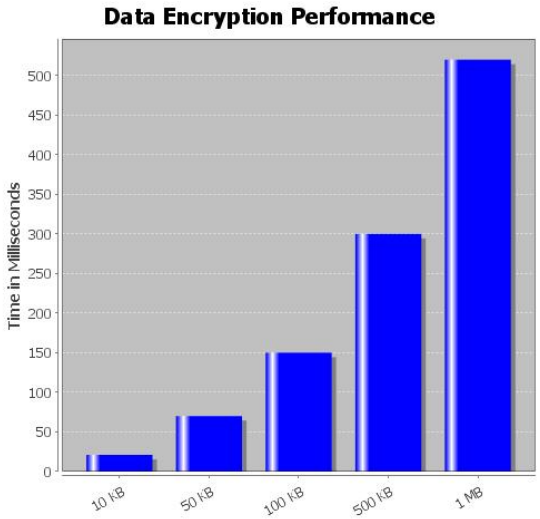


Figure 6 (a): Server Round Performance

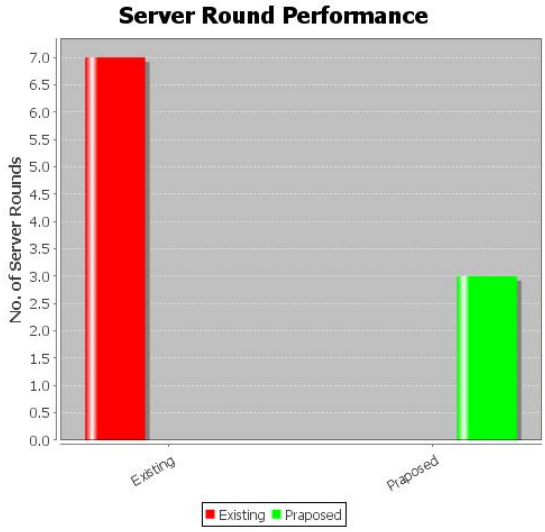


Figure 6 (b): Data Encryption Performance

7. Conclusion

Thus our work is to be extending by imposing various levels of trust upon the two servers and accept a very different method to design the protocol at the age of technical level. Offline dictionary attacks controlled by adversaries for Password Authentication Key Exchange (PAKE) protocol system is applied to secure the connection. The proposed system, is password only system where public key is not required and no PKI. In this project, two basic server models are used to build the architecture, which is used a particular solo back-end server associate with various front-end servers and fascinating applications in federated enterprises. To provide the more security we use SMS integration API for two step verification like Gmail. Distributed file systems in production systems strongly depend on a central node for chunk reallocation. This dependence is clearly incompetent

in a large-scale, failure-prone environment because the central load balancer is put under considerable workload that is linearly scaled withthe system size, and possibly it will become the performance bottleneck and the single point of failure.

8. Future Scope

In future for the database servers we can use cloud or Hadoop servers for more security , as well as the data can be distributed in different chunks with HDFS (Hadoop Distributed File System).

References

[1] Efficient Two-Server Password-Only Authenticated Key Exchange Xun Yi, San Ling, and Huaxiong Wang IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013
[2] L. Barolli and F. Xhafa, JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing, IEEE Trans. Ind. Electron., vol. 58, no. 6, pp. 21632172, Oct. 2010.
[3] Sonal C. Pansare and Prof.Vaishali Nandedkar, "An Efficient Two-Server Password Only Authenticated Key Exchange Secure Against Dictionary Attacks", International Journal of Innovative Research in Computer and Communication Engineering *(An ISO 3297: 2007 Certified Organization)* Vol. 2, Issue 11, November 2014.
[4] X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li, Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793800, Feb. 2010.
[5] M. Cheminod, A. Pironti, and R. Sisto, Formal vulnerability analysis of a security system for remote fieldbus access, IEEE Trans. Ind. Inf., vol. 7, no. 1, pp. 3040, Feb. 2011.
[6] X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li, Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793800, Feb. 2010.
[7] W. Juang, S. Chen, and H. Liaw, Robust and efficient password authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 25512556, Jun. 2008.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] Wei-Kuo Chiang and Jian-Hao Chen, "TW-KEAP: An Efficient Four- Party Key Exchange Protocol for End-to-End Communications", Proceedings of the 4th international conference on Security of information and networks, pp. 167-174, 2011.
[15] Miss. Sonal Chandrakant Pansare and Prof. Vaishali Nandedkar (Assistant Professor), "PAKETS : Password Authenticate Key Exchange using Two–Servers", 2012. cPGCON 2015, MET's Institute of Engineering.

Author Profile

Miss. Sonal Chandrakant Pansare is a student of Masters in Engineering, Computer Department, PVPIT ,Pune University. She received Bachelors of Engineering in 2010 from Mumbai University. Her research interests are Computer Networks (Wireless Networks), Web 2.0, Network Security, Database Systems etc.

Prof. V. S. Nandedkar is working as Assistant Professor and Head of Department of Information Technology in PVPIT, Pune University. She Completed her master in engineering (CSE) with specialisation Signal Processing and now she is perusing her Ph.D.