ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

DESIGN MODEL FOR TWO SERVER PASSWORD ONLY AUTHENTICATED PROTOCOL

Mr. Nishikant Burande *[1], Mr. Kahate S.A.[2]
[*1]Computer Engineering Dept., SPCOE Otur, India
[2]Computer Engineering Dept., SPCOE Otur, India

Keywords: Diffie-Hellman, Elgamal Encryption, PAKE, Periodic Backup

ABSTRACT
It is very unsecure when one server is used for the authentication purpose, as if there is one server all stored passwords can be easily hacked by attacker or dictionary attack may happen. The stored information can be stolen by the hacker, so its need for any alternative method one of the methods is to use two servers for the authentication purpose. In this paper described a design model for two server password only authenticated protocol. Basically used Diffie-Hellman and Elgamal encryption scheme. Also backup facility also provided here. As two types of technique are there one is Symmetric and another one is Asymmetric. In this paper used symmetric Method. Symmetric in the sense that two server equally contribute to each other for the authentication purpose. Here it is very important to note that if one server fails or shut down due to some reason then another server should continue to provide services to the clients. It is a web based approach.

INTRODUCTION
Basically human beings use the low entropy or simple password that is easily remembered. But this leads to hacking easy for the hacker. Dictionary attack also done on that such system. Here PKI model used. PKI is the public key encryption. Asymmetric system is the system in which one server helps to another server for the authentication purpose on the other hand symmetric server, two servers equally co-operate to each other for the authentication purpose. This model uses the Diffie Hellman and Elgamal encryption scheme. Now a days basically two strategies used for the authentication purpose in first client keeps servers public key in addition of password in second method client keeps password only as a secrete key. At the client side both the encryption and decryption keys are generated and sent towards servers through two different two secure channels.

This system can be applied for distributed system where multiple servers exist. But objective is to provide the system with two servers. This system is very secure and robust. The system is secure against active and passive attack also. Here consider client C is associated with server A and Server B. client C creates encryption and decryption keys and sent to both the servers through two secure channels. This is important to note that when authentication the client keeps the servers public key in addition to password. Also there is no restriction for client to amount of information to store on that. Here also considered for the backup server utility as the backup of Server A is stored on Server B and vice versa. If at certain condition one of the servers fails of shutdown due to some reason then another server should continue to provide services to the client. This is new approach for this phenomenon. This is extension for the existing work.

In two server authentication, client needs to separately register on both the servers. For registering at server B it need the private key. After that user can easily login to system. User also can share the files from one client to another client by provided interface. This way system works. So it is highly impossible for the attacker to attach the system and dictionary attack can be avoided with security.
Here we considered two Server

1) Server A
2) Server B
3) Client C
4) User has to register on the server. For registration at Server B it needs the private key provided by the server A.

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

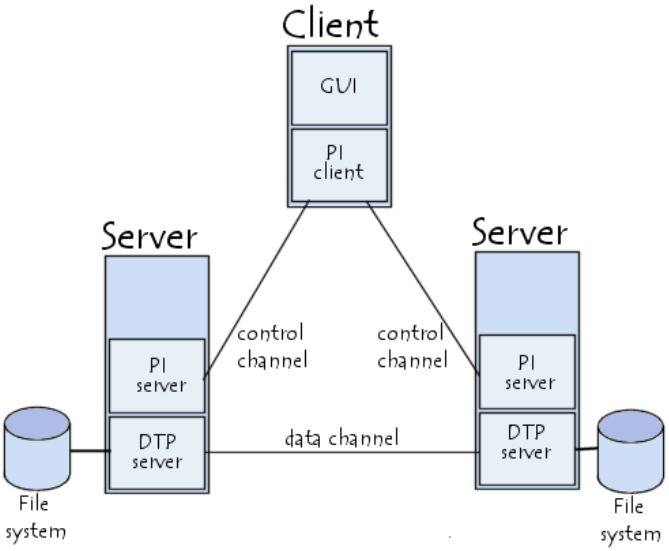

Fig. 1.1 Model for two server authentication

Fig. 1.1.Shows the details model for the two server authentication. File system is also considered because some time needs to share some files from one client to another client. Server A and server B co-operate to each other for the authentication purpose. Security analysis shows that this protocol secure against active and passive attack.

LITERATURE SURVEY

In 2013, Xun Yi, San Ling, and Huaxiong[1] Wang has provided a Efficient two server protocol for security purpose. They provided symmetric solution for the two server authentication purpose. In 2011 Maryam saeed provided two serverautheticaion solution, without use of public key of the server. But after that PAKE1 and PAKE2 provided the solution with less communication rounds and remarkable computational efficiency [3].
In[3] it is also provided that Hitchcock al's protocol is vulnerable to emphemeral key compromise impormasation, offline dictionary attack.

Songs [2] in 2010 provided a security technique and key establishment technique with smartcard which attempts to solve some weaknesses which are found in scheme proposed by Xu, Zhu and Feng[4]. In 2009, Lee et al. showed that Juang et al's scheme is not secure against stolen verifier attack. Users anonymity is not satisfied by Juang Et Al.'s protocol.

Password-authenticated secret sharing (PASS), first found by Bagherzandi et al. [5] at CCS 2011, allow users to distribute among servers. So that the data can be recovered using a single human-memorable password, but no single server (or even no collusion of servers p to a certain size). Next in 2012 2PASS protocol and prove that it meets definition. Given the strong security gurantees, this protocol surprisingly efficient. In its most efficient instantiation under the DDH assumption in the random oracle model [6].

TW-KEAP is an efficient protocol for sharing a session key to protect communication in an insecure network. It is based on the concept of the Diffie-Hellman key exchange protocol which allows the key exchange without session key appearing in the message. The TW-KEAP could support lawful interception because the corresponding server is involved in the key exchange procedure to derive the session key [7]. The concepts in this model comprises pseudonyms, attribute-based authentication, as well as conditional release of information. As a result, the model can express the relevant primitives for privacy-preserving authentication and accountability at the same time[8].

Many solutions exist for authentication, ranging from simple static passwords stored on a single machine to complicated distributed systems. Organizations concerned about protecting their digital assets from

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

sophisticated cyber-attacks have begun relying on two-factor authentication as a defense against unauthorized access [9]. These protocols were proven secure in the random oracle model. Katz, Ostrovsky, and Yung (KOY) [10] demonstrated the first efficient PAKE protocol with a proof of security in the standard model. It also achieves mutual authentication in three rounds. In their work [11], Groce and Katz mentioned their framework will significantly improve efficiency when basing the protocol on lattice assumptions. Katz and Vaikuntanathan [12] first instantiated the KOY/GL PAKE protocol under lattice assumptions. The most technically difficult aspect of their work is the construction of a lattice-based CCA-secure encryption scheme with an associated approximate smooth projective hash system. In order to plug into the JG/GK's framework, we use an approximate lattice-based SPH and an error correcting code (ECC) to do the job of an exact lattice-based SPH.

PROPOSED MODEL

Here proposed a model which symmetric in the sense that two server equally contribute to each other for authentication purpose for client.

Following are the steps for login and registration

1. Registration on Server A
2. Registration on Server B
3. User can Login to System
4. User can Share File for another Users
5. Logout

Step1:

Registration Phase on Server A: While registering at Server A, user have to register with basic details.

Step2:

Registration Phase on Server B: While registering at Server B, user have to provide private key of Server A.

Step3:

Verification: At this step User is verified with credentials from Server A and Server B.

Step4:

After verification user can easily login to the system. If require user can share file.

CONCLUSION

Here proposed a basic two server efficient protocol for the increase security in authentication. Many protocols have been proposed from long ago. Here taken approach suppose one server shut down or fails then another server can continue to provide services to the clients. This protocol is secure against active and passive attack.

REFERENCES

1. Xun Yi, San Ling, and Huaxiong Wang, " Efficient Two Server Password-Only Authenticated Key Exchange" IEEE Transactions on Parallel and Distributed System Vol-24 No: 9 Year 2013
2. Juan E. Tapiador, Julio C. Hernandez-Castro, "Cryptanalysis of Song's advanced smart card based password authentication protocol", 2010. Online available: http://arxiv.org/pdf/1111.2744.pdf
3. Maryam Saeed, HadiShahriarShahhoseini, "An Improved two-party Password Authenticated Key Exchange Protocol without Server's Public Key", IEEE 3rd International Conference on Communication Software and networks (ICCSN-2011), pp. 90-95, 2011.
4. J. Xu, W.-T Zhu, and D.-G Feng. "An improved smart card based password authentication scheme withprovable security." Computer Stan- dards& Interfaces 31, pp. 723–728, 2009.
5. AmuthaPrabakarMuniyandi, RajaramRamasamy, "Password Based Remote Authentication Scheme using ECC for Smart Card", Proceedings of the 2011 International Conference on Communication, Computing & Security, pp. 549-554, 201
6. An Camenisch, Anna Lysyanskaya, "Practical Yet UniversallyComposable Two-Server Password Authenticated Secret Sharing", Proceedings of the 2012 ACM conference on Computer and communications security, pp. 525-536, 2012.
7. Wei-Kuo Chiang and Jian-HaoChen, "TW-KEAP: An Efficient Four-Party Key Exchange Protocolfor End-to-End Communications", Proceedings of the 4th international conference on Security of information and networks, pp. 167-174, 2011.
8. PatrikBichsel, Jan Camenisch, "A Calculus for Privacy friendly Authentication", Proceedings of the 17th ACM symposium on Access Control Models and Technologies, pp. 157-166, 2012.

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

9. Matthew A. Ezell, Gary L. Rogers, "A Framework for Federated Two-Factor Authentication Enabling Cost Effective Secure Access to Distributed Cyberinfrastructure", Proceedings of the 1st Conference of the Extreme Science and Engineering Discovery Environment: Bridging from the eXtreme to the campus and beyond, article no 7, 2012.
10. J. Katz, R. Ostrovsky, and M. Yung "Efficient and Secure Authenticated Key Exchange Using Weak asswords". Journal of the ACM, Vol. 57, issue 1, pp. 78–116, 2009.
11. A. Groce, J. Katz "A New Framework For Efficient Password-based Authenticated Key Exchange", In proceedings of 17th ACM Conference on Computer and Communications Security, pp. 516–525. ACM Press, New York, 2010.
12. J. Katz and V. Vaikuntanathan "Password-based Authenticated Key Exchange Based on Lattices", In Advances in Cryptology, volume 5912 of LNCS, pp. 636–652.Springer, 2009.