{tag} {/tag}

IJCA Proceedings on International Conference on Innovations in Computing Techniques (ICICT 2015)

ICICT 2015 - Number 2

Year of Publication: 2015

Authors:
Anitha Kumari K

Sudha Sadasivam G

Rohini L

{bibtex}icict1473.bib{/bibtex}

Abstract

In real time applications, more number of servers and data centers are needed for fast processing in the required time and to provide high level of security in communication due to rapid growth of data. Password Authenticated Key Exchange (PAKE) protocol is used to verify the authentication of the communicating parties and then secret key is generated based on their passwords. Mostly in single server environment the users share a password with a trusted

single server. If the single server is compromised, then the environment is prone to many attacks such as online dictionary attacks, server spoofing attack and stolen verification attacks. The proposed system is built based on ElGamal encryption scheme and Diffie-Hellman Key Exchange algorithm in the two-server password based authentication and key exchange protocol. Discrete logarithm in f*p is used in ElGamal encryption to provide additional security. Discrete logarithm problem would render the ElGamal cryptosystem, secure against the man in the middle attack and other cryptographic attacks. The proposed scheme is provided with additional security and also its resistance against attacks.

References

- Xun Yi. , and San Ling, Huaxiomg, "Efficient Two-Server Password Only Authenticated Key Exchange", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1773- 1782, 2013.
- Hung-Yu Chien. , and Tzong-Chen Wu, Ming- KueiYeh, "Provably Secure Gateway-Oriented Password-Based Authenticated Key Exchange Protocol Resistant to Password Guessing Attacks",Journal Of Information Science And Engineering, Vol. 29, No. 2, pp. 249-265, 2013.
- Yanjiang Yang. , and Deng R. H, FengBao, "A Practical Password-Based Two-Server Authentication and Key Exchange System", IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 2, pp. 105-114, 2006.
- Jun Ho Lee. , and Dong Hoon Lee, "Secure and Efficient Password-Based Authenticated Key Exchange Protocol for Two-Server Architecture", International Conference on Convergence Information Technology, 2007, Vol. 21, No. 23, pp. 2102-2107, 2007.
- Dexin Yang. , and Bo Yang, "A Novel Two-Server Password Authentication Scheme with Provable Security", IEEE 10th International Conference on Computer and Information Technology (CIT), pp. 1605-1609, 2010.
- Her-TyanYeh. , and Hung-Min Sun, "Simple Authenticated Key Agreement Protocol Resistant to Password Guessing Attack", ACM SIGOPS Operating Systems Review, Vol. 36, No. 4, pp. 14-22, 2002.
- Anamika Chouskey. , and YogadharPandey, "An Efficient Password Based Two-Server Authentication and Pre-shared Key Exchange System using Smart Cards", International Journal of Computer Science and Information Technologies,Vol. 4, No. 1, pp. 117-120, 2013.
- Katz J. , and MacKenzie P, Taban G, Gligor V, "Two-server password-only authenticated key exchange", Proc. ACNS'05, pp. 1-16, 2009.
- Lishan Kang, Xuejie Zhang(2010), "Identity - Based Authentication in Grid Storage Sharing", 2010 International Conference on Multimedia Information Networking and Security.
- Dinesha H A, Agrawal V K, "Multi-Dimensional Password Generation Technique for Accessing Cloud Services", International Journal on Cloud Computing: Services and Architecture, 2012, Vol. 2, No. 3. pp. 31.
- Bhavana A, Alekhya V, Deepak K, and Sreenivas V, "Password Authentication

System (PAS) for Cloud Environment", International Journal of Advanced Computer Science and Information Technology, 2013, Volume 2, pp. 29-33.

Index Terms

Computer Science Security

Keywords

Password Authenticated Key Exchange Two-server Diffie-hellman Key Exchange.