IJARES/September 2014/Volume-2/Issue-9/1452-1457 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

MANAGING OF AUTHENTICATING PASSWORD BY MEANS OF NUMEROUS SERVERS

Kanchupati Kondaiah[1], B.Sudhakar[2]

[1]M.Tech Student, Dept of CSE, Audisankara College of Engineering & Technology, Gudur, A.P, India

[2]Associate Professor, Dept of CSE, Audisankara College of Engineering & Technology, Gudur, A.P, India

ABSTRACT:

Modern research progress in password-based validation has approved a client as well as a server usually to authenticate by means of password and for the meantime to set up cryptographic key in support of safe communications subsequent to authentication. We put forward a novel symmetric two-server password authenticated key exchange procedure which supports two servers to calculate in parallel and for the meantime keeps effectiveness for practical use. Novel symmetric solution is additionally competent than active symmetric two-server password authenticated key exchange procedure. In our procedure, the client as well as the two servers converse all the way through a public channel which might be eavesdropped, replayed, as well as even tampered by an attacker. Security analysis has exposed that our procedure is protected against passive in addition to active attacks in situation where single server is compromised.

Keywords: Cryptographic key, Security, Public channel, Attacker, Password authenticated key exchange.

1. INTRODUCTION:

Representative protocols in support of password-based authentication assume a single server storing the entire passwords essential to substantiate clients. A large part of user-chosen passwords are readily guessed by design [1]. Previous password-based authentication schemes transmitted a cryptographic hash of password on public channel which build hash value available towards an attacker. When this is completed,

and it is extremely general, the attackers can effort offline, quickly testing probable passwords against accurate password's hash value. Present solutions in support of password based authentication go after two models such as PKI-based representation which assumes that the client maintain server's public key besides sharing a password with server. In this situation, the client can transmit password towards server by public key encryption. The second representation is described as password-only representation. Present solutions in support of two-server password authenticated key exchange are additionally symmetric in logic that two peer servers evenly add to authentication, or else asymmetric in sense that one server validates the client with the aid of an additional server. A symmetric two server password authenticated key exchange procedure can run in parallel as well as establishes secret session keys among client and two servers, correspondingly. In case one of two servers shuts down due to denial-of-service attack, an additional server can carry on to make available services to authentic clients. Fig1 shows the two server system [2][3]. Present asymmetric procedures require two servers to exchange messages for quite a lot of times. These asymmetric mythologies are minor competent than a symmetric design which permits two servers to work out in parallel. We put forward a novel symmetric two-server password authenticated key exchange procedure which supports two servers to calculate in parallel and for the meantime keeps effectiveness for practical use [4].

2. METHODOLOGY:

Up to date research progress in password-based validation has approved a client as well as a server usually to authenticate by means of password and for the meantime to set up cryptographic key in support of safe communications subsequent to authentication. We put forward a novel symmetric solution for two-server password authenticated key exchange. Even though we make use of notion of public key cryptosystem, our procedure follows password-only representation. The encryption as well as decryption key pairs in support of two servers are generated by client and delivered towards servers all the way through dissimilar secure channels throughout client registration, as client in any two-server password authenticated key exchange procedure sends two halves of password in the direction of two servers in

secret [6][7]. Novel symmetric solution can be functional in distributed systems where numerous servers exist. Our procedure is symmetric if two peer servers evenly put in towards authentication in terms of computation as well as communication. Novel symmetric solution desires four communication rounds for client as well as two servers equally to validate and concurrently to set up secret session keys. Novel symmetric solution is additionally competent than active symmetric two-server password authenticated key exchange procedure. In terms of parallel working out, our procedure is still more competent to existing asymmetric two-server password authenticated key exchange procedure. In two-server password authenticated key exchange procedure, there exist two servers as well as a group of clients. The two servers assist to validate clients and make available services towards authentic clients. An adversary in our system is moreover passive or else active. We consider mutually online dictionary attack, where an attacker effort to login constantly, trying each probable password, as well as offline dictionary attack, where an adversary obtain information concerning password from experiential transcripts concerning sessions of log. The attack of online dictionary was not averted by cryptographic way however can be effortlessly noticed and suspended once verification fails quite a lot of times [8][9]. We suppose that an adversary can compromise single server only and get hold of all information accumulated in server. A passive adversary is capable to observe the communications between clients as well as two servers. Security analysis has exposed that our procedure is protected against passive in addition to active attacks in situation where individual server is compromised. An active adversary is capable to act as to be both one server and client to converse with truthful server or imagine being both two servers to converse with lawful client, diverge in an arbitrary method from actions approved by procedure. In our procedure, the client as well as the two servers converse all the way through a public channel which might be eavesdropped, replayed, as well as even tampered by an attacker. Our procedure is symmetric if two peer servers evenly put in towards authentication in terms of computation as well as communication. In our procedure, the adversary efforts to become skilled at the undisclosed session key established among the client as well as

truthful server [10]. In active attack, adversary gain knowledge of the secret session key among client and honest server if adversary can conclude password of client.

3. RESULTS:

We put forward a novel symmetric solution for two-server password authenticated key exchange. Even though we make use of notion of public key cryptosystem, our procedure follows password-only representation. Security analysis has exposed that our procedure is protected against passive in addition to active attacks in situation that individual server is compromised. Performance examination has exposed that introduced method is well-organized than existing symmetric as well as asymmetric two-server password authenticated key exchange procedures in terms of parallel computation. Novel symmetric solution desires four communication rounds for client as well as two servers equally to validate and concurrently to set up secret session keys. Novel symmetric solution is additionally competent than active symmetric two-server password authenticated key exchange procedure. In terms of parallel working out, our procedure is still more competent to existing asymmetric two-server password authenticated key exchange procedure.

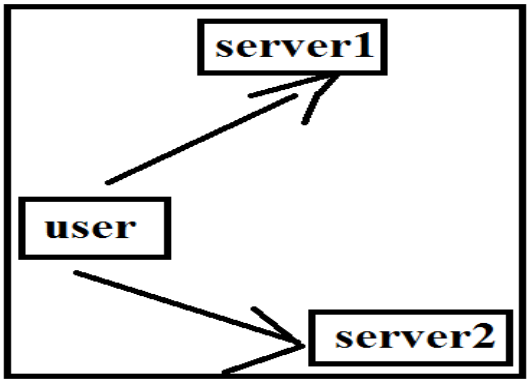

Fig1: An overview of Two Server System

4. CONCLUSION:

Previous password-based authentication schemes transmitted a cryptographic hash of password on public channel which build hash value available towards an attacker. Present solutions in support of two-server password authenticated key exchange are additionally symmetric in logic that two peer servers evenly add to authentication, or else asymmetric in sense that one server validates the client with the aid of an additional server. We put forward a novel symmetric two-server password authenticated key exchange procedure which supports two servers to calculate in parallel and for the meantime keeps effectiveness for practical use. A symmetric two server

password authenticated key exchange procedure can run in parallel as well as establishes secret session keys among client and two servers, correspondingly. An active adversary is capable to act as to be both one server and client to converse with truthful server or imagine being both two servers to converse with lawful client, diverge in an arbitrary method from actions approved by procedure. In our procedure, the adversary efforts to become skilled at the undisclosed session key established among the client as well as truthful server. The encryption as well as decryption key pairs in support of two servers are generated by client and delivered towards servers all the way through dissimilar secure channels throughout client registration, as client in any two-server password authenticated key exchange procedure sends two halves of password in the direction of two servers in secret. In two-server password authenticated key exchange procedure, there exist two servers which assist to validate clients and make available services towards authentic clients. Performance analysis has shown that our procedure is well-organized than existing symmetric as well as asymmetric two-server password authenticated key exchange procedures in terms of parallel computation.

REFERENCES

[1] V. Boyko, P. Mackenzie, and S. Patel, "Provably Secure Password- Authenticated Key Exchange Using Diffie-Hellman," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 156-171, 2000.

[2] 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.

[3] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, IT-22, no. 6, pp. 644-654, Nov. 1976.

[4] 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.

[5] 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.

[6] W. Ford and B.S. Kaliski Jr., "Server-Assisted Generation of a Strong Secret from a Password," Proc. IEEE Ninth Int'l Workshop Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 176-180, 2000.

[7] O. Goldreich and Y. Lindell, "Session-Key Generation using Human Passwords Only," Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (Crypto '01), pp. 408-432, 2001.

[8] L. Gong, T.M.A. Lomas, R.M. Needham, and J.H. Saltzer, "Protecting Poorly-Chosen Secret from Guessing Attacks," IEEE J. Selected Areas in Comm., vol. 11, no. 5, pp. 648-656, June 1993.

[9] S. Halevi and H. Krawczyk, "Public-Key Cryptography and Password Protocols," ACM Trans. Information and System Security, vol. 2, no. 3, pp. 230-268, 1999.

[10] D. Jablon, "Password Authentication Using Multiple Servers," Proc. Conf. Topics in Cryptology: The Cryptographer's Track at RSA (RSA-CT '01), pp. 344-360, 2001.

[11] T.M.A. Lomas, L. Gong, J.H. Saltzer, and R.M. Needham, "Reducing Risks from Poorly-Chosen Keys," ACM Operating Systems Rev., vol. 23, no. 5, pp. 14-18, 1989.

[12] P. MacKenzie, S. Patel, and R. Swaminathan, "Password-Authenticated Key Exchange Based on RSA," Proc. Sixth Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt '00), pp. 599-613, 2000.

[13] P. Mackenize, T. Shrimpton, and M. Jakobsson, "Threshold Password-Authenticated key Exchange," Proc. 22nd Ann. Int'lCryptology Conf. (Crypto '02), pp. 385-400, 2002.

[14] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.