Efficient Multi-Server Password Authenticated Key Agreement

M.Srikanth[1],K.Sivani[2], T.Aparna[3], SK .Mehatab[4], R.Halok Nath[5].
[1]*Asst. Prof, CSE, Tirumala Engineering College, Narasaraopet.*
[2, 3, 4, 5] *B. Tech Students, Tirumala Engineering College, Narasaraopet.*

Abstract: Since the number of server providing the facilities for the user is usually more than one, the authentication protocols for multi-server environment are required for practical applications. Most of password authentication schemes for multi-server environment are based on static ID, so the adversary can use this information to trace and identify the user's requests. It is unfavourable to be applied to special applications, such as ecommerce. In this paper, we develop a secure dynamic ID based remote user authentication scheme to achieve user's anonymity. The proposed scheme only uses hashing functions to implement a robust authentication scheme for the multi-server environment. It provides a secure method to update password without the help of third trusted party. The proposed scheme does not only satisfy all requirements for multi-server environment but also achieve efficient computation. Besides, our scheme provides complete functionality to suit with the real applications.

1. INTRODUCTION

With the rapid growth of Internet technologies, the system providing resources to be accessed over the network often consists of many different servers around the world. The distribution of the remote system hardware in different places makes the user access the resources more efficiently and conveniently. In a single server environment, the issue of remote login authentication with the smart card has already been solved by a variety of schemes. If conventional password authentication methods are applied to multi-servers environment, each network user does not only need to log into various remote servers repetitively but also need to remember many sets of identities and passwords. It is inefficient and easily leads to the compromise of the identities and passwords. Besides, it is an important topic for managing the shared secret key efficientlyamong the involved participants. On the other hand, with the rapid growth of those e-commerce applications, a remote user authentication with anonymity is required or desirable. Until now, several papers have been devoted to the study of accessing the resources of multi-servers environments. Among these schemes, based on the computation complexity, the smart card-based authentication schemes are divided into two types, namely hash-based authentication and public-key based authentication. A secure and efficient remote user authentication for multiserver environment usually meets the following requirements:

A secure and efficient remote user authentication for multiserver environment usually meets the following requirements:

1.1. Single Registration:

It allows the user to register only once at the registration center and then he can access all the registered servers.

1.2. Low Computation

Due to the computation power constraints of smart card, they may not provide a powerful computation capability.

1.3. No Verification Table

It needs no password tables or verification tables are stored in each registered server.

1.4. Update Password Securely and Freely

It allows the cardholder to update his password freely after assuring the legality of cardholder.

1.5. Mutual Authentication and Key Agreement

It allows the users and servers to authenticate each other and then negotiate a session key to protect the transmitting message.

1.6. Security

The authentication scheme must be able to resist all kinds of attacks such that it can be applied in the real world. In this paper, we present a secure and efficient authentication scheme with anonymity for multi-server environment. The objective of our scheme emphasize that it does not only satisfy the all above requirements but also protect the user's identity to apply to the special service, such as e-economic applications. Our scheme can get service granted from multi-server environment without maintaining any secret key tables in each registered server.

2. LITERATURE REVIEW:

Due to the widespread applications of Internet services, the study of accessing the resources of multi-server environment has received considerable attention, and many schemes are proposed successively. Those schemes can be dived into two types, namely hash-based authentication and public-key based authentication. Lee and Chang (2000) proposed a user identification and key distribution scheme that is based on the difficulty of factorization and hash function. It agreed with the multiserver environment. Next, Tsaur (2001) proposed a remote user authentication scheme based on RSA cryptosystem and Lagrange interpolating polynomial for multi-server environments in the same time, Li et al. proposed a remote password authentication scheme by using neural networks. However, it is impractical to spend too much time and cost on training and maintaining neural networks.

3. PROPOSED AUNTHENTICATION PROTOCOL:

In this section, we propose an efficient and secure authentication scheme for multi-server environment. . In view of the efficiency computation, the proposed scheme use simple hashing functions to complete the mutual authentication and session key agreement. Consider the multiserver environment containing three participants, the user (Ui), the service provider (Sj) and the registration center (RC). It is assumed that RC is a trusted party responsible for the secret keys distribution between Ui and Sj.

Different phase works as follows:

3.1. Registration Phase

When the user Ui wants to access the resources of the service provider Sj, he has to submit his identity IDi and password PWi.

Definition of notations used in our scheme

Ui	ith user.
Sj	jth server .
RC	Registration center.
IDi	Unique identification of Ui .
PWi	Unique password of Ui .
SIDj	Unique identification of Sj.
CIDi	Dynamic ID of Ui.
h(.)	A one-way hash function x.
X	The master secret key of registration center .
Y	A secret number shared with the registration center and all servers.
$\oplus$	The exclusive-or operation .
||	The concatenation operation.

3.2. Login Phase

The userUi keys his identity IDi , password PWi and the server identity SIDj in order to login the service provider Sj.

3.3. Password Change Phase

When the userUi wants to update his password without the help of RC, he inserts his smart card to card reader and inputs (IDi , PWi) corresponding to the smart card.

4. SECURITY ANALYSIS:

4.1. Two-Factor Security

Obviously, if both the user's smart card and his password were stolen, then there is no way to prevent the attacker from masquerading as the user. So the best we can do is to guarantee the security of the scheme when either the user's smart card or his password is stolen, but not both. This security property is called two-factor security.

4.2. Replay Attack

The replay attack is replaying the same message of the receiver or the sender again.

4.3. Server Spoofing Attack

Our scheme can protect the user from cheating by the masqueraded service provider since the adversary cannot construct thesession key SK without the knowledge of Bi and y. After communicating with the masqueraded service provider, the legal user can detect immediately and terminate the session.

4.4. Insider And Stolen Verifier Attack

The insider attack is defined that any manager of system purposely leaks the secret information, and then lead to serious security flaws of authentication scheme.Our scheme also does not maintain any verifier table. Thus the insider and stolen verifier attack are resisted.

4.5. Known–Key Security

The known-key security means that compromise of a past session key cannot derive any further session key.

4.6. Forward Secrecy

The forward secrecy means that even though the master secret key x is disclosed for some reason, it will not cause the compromise of any earlier session.

4.7. User Anonymity Protected

Thus, the attacker may incept and analyze the login message. It is infeasible to derive IDi from the login message. Moreover, the login message is dynamic in each login. Among the parameters of login message, CIDi is associated with nonce Ni and dynamically changed.

4.8. Securely Chosen Password

In the password change phase, the cardholder can freely change password as his favorite stings without the help of RC. To avoid unauthorized users easily changing the password after obtaining the smart card for some reason, the legality of the cardholder must be assured.

5. PERFORMANCE AND FUNCTIONALITY ANALYSIS:

In general, the efficiency evolution usually is divided into communication cost and computation cost,We use the following facts and assumptions to evaluate. Assume the identity IDi, password PWi, timestamp and nonces are all 128-bit length; the large prime in modular operation is 1024-bit length in practical implementation. Moreover, we also assume both the output size of secure one-way hashing functions h(.) and the block size of secure symmetric cryptosystem are 128-bit. The notations Th, Tsym and Texp are defined as the time complexity for hashing function, symmetric encryption/decryption and exponential operation respectively.

6. CONCLUSION:

We demonstrate that our scheme can satisfy all of the essential requirements. Our scheme does not only manage the secret key tables associated with the users but also achieve user's anonymity. Moreover, our scheme only uses hashing functions to implement mutual verification and session key agreement. It is well suited to the smart card's applications.

REFERENCES

[1] C.C. Chang, T.C. Wu, Remote password authentication with smart cards, IEE Proc. E 138 (3) (1991) 165–168.

[2] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 46 (1) (2000) 28–30.

[3] H.M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 46 (4) (2000) 958–961.

[4] K. Chan, Li M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 46 (2000) 992–993.

[5] [5] J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 49 (2) (2003) 414–416.

[6] K.C. Leung, L.M. Cheng, A.S. Fong, C.K. Chan, Cryptanalysis of a modified remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 49 (4) (2003) 1243–1245.

[7] Amit K. Awashti, Sunder Lal, An enhanced remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 50 (2) (2004) 583–586.

[8] C. Chang, K.F. Hwang, Some forgery attacks on a remote user authentication scheme using smart cards, Informatics 14 (3) (2003) 289–294.

[9] M.L. Das, A. Saxena, V.P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Trans. Consum. Electron. 50 (2) (2004) 629–631.

[10] K. Awasthi, Comment on a dynamic ID-based remote user authentication scheme, Trans. Cryptol. 01 (2) (2004) 15–16.

[11] W.C. Ku, S.T. Chang, Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards, IEICE Trans. Commun. (5) (2005).

[12] J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 49 (2) (2003) 414–416.

[13] C. Lee, M.S. Hwang, W.P. Yang, A flexible remote user authentication scheme using smart cards, ACM Oper. Syst. Rev. 36 (3) (2002) 46–52.

[14] W.B. Lee, C.C. Chang, User identification and key distribution maintaining anonymity for distributed computer network, Comput. Syst. Sci. 15 (4) (2000) 211–214.

[15] W.J. Tsuar, C.C. Wu, W.B. Lee, A flexible user authentication for multiserver internet services, Networking-JCN2001LNCS, vol. 2093, SpringerVerlag, 2001, pp. 174–183.

[16] L. Li, I. Lin, M. Hwang, A remote password authentication scheme for multi-server architecture using neural networks, IEEE Trans. Neural Netw. 12 (6) (2001)1498–1504.

[17] C. Lin, M.S. Hwang, L.H. Li, A new remote user authentication scheme for multi-server architecture, Future Gener. Comput. Syst. 1 (19) (2003) 13–22.

[18] W.J. Tsuar, An enhanced user authentication scheme for multi-server internet services, Appl. Math. Comput. 170 (2005) 258–266.

[19] T.S. Wu, C.L. Hsu, Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks, Comput. Secur. 23 (2004) 120–125.

[20] Y. Yang, S. Wang, F. Bao, J. Wang, R. Deng, New efficient user identification and key distribution scheme providing enhanced security, Comput. Secur. 23 (8) (2004) 697–704.

[21] W.S. Juang, Efficient multi-server password authenticated key agreement using smart cards, IEEE Trans. Consum. Electron. 50 (1) (2004) 251–255.

[22] C. Chang, J.S. Lee, An efficient and secure multi-server password authentication scheme using smart cards, IEEE. Proceeding of the International Conference on Cyberworlds, 2004.

[23] C. Chang, J.Y. Kuo, An efficient multi-server password authenticated keys

agreement scheme using smart cards with access control, IEEE. Proceeding of the 19th International Conference on Advanced Information Networking and Applications, 2005.

[24] X. T, R.W. Zhu, D.S. Wong, Improved efficient remote user authentication schemes, Int. J. Netw. Secur. 4 (2) (2007) 149–154.

[25] T.S. Messergers, E.A. Dabbish, R.H. Sloan, Examining smart card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552. [26] A. Menezes, O.P. Van, S. Vanstone, Handbook of applied cryptography, CRC Press, LLC, Boca Raton, 1997.