DESIDOC Journal of Library & Information Technology, Vol. 29, No. 3, May 2009, pp. 49-54

© 2009, DESIDOC

Secure Authenticated Key Exchange Protocol for Credential Services

R.Balakrishna[1], U. Rajeswara Rao[2], and N. Geethanjali[2]

[1] *Department of CSE, Don Bosco Institute of Technology, Bangalore-570 064*
[2.] *Department of Mathematics and Computer Science and Technology*
S.K. University, Anantapur-515 003

ABSTRACT

Remote user authentication and key agreement system through smartcard is a viable practical solution to validate the eligibility of a remote user and thus to provide a secure communication. This paper suggests a Secure Authenticated Key Exchange Protocol (SAKEP) for Credential Services. The major intrinsic worth of this scheme include that, the system do not require any verification table and the user is at liberty to choose and change the password. Further, with this system, the computation and communication costs are lower as the scheme adopts one-way hash functions, block ciphers and smartcard. In addition, the proposed scheme offers mutual authentication between the server and the user by a nonce-based plan and is free from time-synchronisation problem. The proposed scheme is secured against Id-theft, also resists to replay attacks, stolen verifier attacks, guessing attacks, reflection attack, and offers forward secrecy and known-key security.

Keywords: Key exchange protocol, KEP, authentication, smartcard, secure, ID-theft

NOMENCLATURE

Ui	:	The user.
IDi	:	The user identity.
PWi	:	The password of Ui.
h (.)	:	A one-way hash function.
Å	:	Bitwise XOR operation.
||	:	Concatenation.
Ek (y)	:	Encryption of y with k.
Dk (y)	:	Decryption of y with k.

1. INTRODUCTION

In the view of rapid advancement and utility of computer network, achieving secrecy and authentication becomes an important requirement so that the user authentication can avoid access to unauthorised network server. When a client choose a service with a server, the transmitted messages between them has to be maintained undisclosed, for which those schemes are built with a session key and get protected so that their subsequent communications becomes secured and protected. The scheme proposed by Lamport[1] to authenticate a remote user over an unsecured channel, and several other such schemes proposed to improve functionality, security and efficiency[2-9, 11,12,14,15] are based on static login-ID which is prone to leak partial information from the user's login message to the adversary. The adversary in turn intercepts the login ID and later manipulates it with other intercepted parameters and forges the login ID. Therefore, employing a dynamic-ID for each login can avoid the risk of ID-theft.

A typical remote authentication scheme consists of a user and a server. Before a new user can use services of the server, the user first has to register at the server to log into server; the user has to submit identity and the corresponding password to the server. The server in turn computes the one-way hashing value of the user's password and compares the same with that stored with in the verification table. The above approach incurs the risk and cost of protecting as well as managing the verification table and will prevent the replay attack.

As a remedy to the above problem, several other authentication schemes without the verification table were proposed[2,3, 5-8, 10, 11, 12, 14] and these schemes possessed inherent disadvantages like difficulty of memorising the server generated random password or a long key. These were effectively addressed by introducing "function to let users freely choose passwords"[2, 5-7,10,11,12,14]. Hang[12] reports several internet frauds occurring due to unilateral

Received on 5 September 2008

authentication. Thus, there is a need for stressing for the mutual authentication between the user and server so as to ensure the security of authentication[2,5,6,9,10,14,15].

The above short comings are effectively addressed by adopting smart cards in network security protocols and also remote user authentication schemes owing to its low cost, portability, efficiency, and the cryptographic capabilities. Further, when these cards are preferred for remote authentication and session key agreement application, the following criterions becomes crucial:

- *C1: No verification table:* No verification or password table is stored in a server.
- *C2: Freely chosen password:* Users can freely choose and change their passwords.
- *C3: Low computation and communication cost:* Due to the power constraints and small flash memory of smart cards, they may not provide a powerful computation capability and high bandwidth.
- *C4: Mutual authentication:* Servers and users can authenticate each other.
- *C5: Session key agreement:* Servers and users must negotiate a session key to be used for protecting their subsequent communications.

In addition, the following few security criteria are also essential for session key agreement[9,10].

- *S1: Session key security:* At the end of the key agreement the session is known only to the user and the server.
- *S2: Forward secrecy:* A compromised long-lived secret key cannot derive the session keys used before.
- *S3: Known-key security:* Only knowing a compromised session key cannot determine the other used session keys.

Chien[4], *et al.* proposed a novel user authentication scheme that satisfied the above criterions except C5 that suffered by a serious time synchronisation problem of the user's time and the server's time to an extent of undesirable range. The improved scheme of Jaung[10] satisfied the session key agreement mechanism. Later in 2004, Das[6], *et al*. came out with dynamic ID-based remote user authentication scheme with unilateral authentication using smartcards. Recently the contributions of Liao[11], *et al*. enhanced the security to the dynamic ID-based remote user authentication scheme that offered mutual authentication. But both the above suffered with non exchangeability of session key. In view of the above discussion, the present study is aimed at proposing an efficient dynamic-ID based password authenticated key agreement system using smart cards which fulfills all criterions mentioned and also the conditions of nonce-base.

2. THE PROPOSED SCHEME

The study proposes the dynamic ID-based password authenticated key agreement using smartcards without time concurrency. The salient features of the proposed scheme are: registration is performed only once; login, mutual authentication and session key exchanges are executed every time as and when the user logs into the system, and change of password may be invoked whenever the user wants to change password.

2.1 Registration Phase

As the user Ui submits identity IDi and chooses password PWi and submits IDi and h (PWi) to the remote system through a secured channel, the remote system performs the following steps:

Computes Ti = h (IDi || x) where x is a secret key of the remote system.

Vi = Ti Å h (IDi || h (PWi))

Bi = h (PWi) Å h(x) and Hi= h (Ti)

The remote system issue a smart card to the user with the secured information {Vi, Bi, Hi, h (.), y} where y is the server's secret.

2.2 Login Phase

As the user Ui inserts smart card into the card reader terminal, upon keying in the identity IDi and password PWi*, the smart card performs the following,

(i) Ti* = Vi Å h (IDi || h (PWi)) and Hi*= h (Ti*). Checks whether Hi* = Hi or not. If yes, the legality of the user can be assured and proceeds to the next step; otherwise, reject the login request.

(ii) Generates a nonce Ni and computes

CIDi = h (PWi) Å h (NiÅ yÅ Ti)

Pi = Ti Å h (NiÅ y)

Qi = h (Bi Å NiÅ y)

(iii) Send a login request message m = {CIDi, Pi, Qi, Ni} to the Server.

2.3 Mutual Authentication and Session Key Exchange Phase

Upon receiving message m {CIDi, Pi, Qi, Ni}, the remote system authenticates the user Ui based on the following steps:

(i) Computes Ti = Pi Å h (NiÅ y), h (PWi) = CIDi Å h (NiÅ yÅ Ti) and Bi = h (PWi) Å h(x).

(ii) Computes h (Bi Å NiÅ y) and then compares it with Qi. If they are not equal, the server rejects the login request and terminates this session.

(iii) Generates a nonce Nj and computes Mi = h (Bi Å Ni Å Nj Å y) and the session key sk = h (Bi ||Ni || Nj || y) and send back the message {Esk (Mi), Nj} to the user Ui. Upon receiving the acknowledgement message. {Esk (Mi), Nj}, the user Ui performs the following steps.

(iv) Computes the session key sk' = h (Bi ||Ni || Nj || y) and checks whether Dsk' (Esk (Mi)) = h (Bi Å Ni Å Nj Å y). If they are equal, Ui confirms that he/she communicates with the valid remote system/server and that the remote system has received sk correctly, otherwise the connection is interrupted.

(v) The user sends Esk (Nj + 1) to the server.

(vi) Upon receiving the reply message the server performs Dsk' (Esk (Nj + 1)) and compares it with Nj + 1. If it holds, the identity of the user is assured and that both the server and the user have agreed on the same session key sk.

2.4 Password Change Phase

This phase may be invoked whenever the user Ui wants to change the password. Further the user can easily change the password without any assistance from the remote system.

The adversary updating passwords freely by stealing smartcard are prevented in this proposed scheme and the steps followed are:

The smartcard first follows the Step 1 of the login phase requests the legality of the card holder by allowing the card holder to resubmit a new password PWinew and then Vi stored in the smartcard will be updated with Vi new = Ti Å h(IDi || h(PWinew)). Similarly, Bi stored in the smartcard will be replaced with

Binew=BiÅ h (PWi) Å h (PWinew), which yields h (PWinew) Å h(x). Thus the password has been changed with the new password PWinew and terminates the operation thus rejecting the smart card.

3. SECURITY ANALYSIS OF THE PROPOSED SCHEME

Security analysis of the proposed scheme for various attacks are:

3.1 Password Guessing Attacks

The proposed scheme provides a shield against the password guessing attack and is confirmed as follows:

Let the impersonate guesses Ui's password and is PW*, the mutual authentication phase is performed as follows.

The smartcard generates nonce Ni and computes

CIDi = h (PW*) Å h (NiÅ yÅ Ti)

Pi = Ti Å h (NiÅ y)

Qi = h (Bi Å NiÅ y) and sends a login request message m = {CIDi, Pi, Qi, Ni} to the server. After getting the message, S computes Ti = Pi Å h(NiÅ y), h(PW*) = CIDi Å h(NiÅ yÅ Ti) and Bi = h(PW*) Å h(x). Computes h (Bi Å NiÅ y) and then compares it with Qi.. However, these two must be unequal as Bi = h (PWi) Å h(x) "' h (PW*) Å h(x). So, S can detect on-line password guessing attack.

3.2 Replay Attacks

The replay attack is replaying the same message of the receiver or the sender again and again. This proposed scheme uses nonce to withstand replay attacks and is confirmed as follows. After intercepting the previous login request {CIDi, Pi, Qi, Ni} from the user Ui, the attacker may replay the message to the server. Then the attacker can receive acknowledgement message {Esk (Mi), Nj} from the server after Step3 of mutual verification phase. However, the attacker cannot compute sk without knowing Bi and y. Similarly, when we assume that the attacker replies a previous message {Esk (Mi), Nj} to Ui, where Mi is associated with N1. Upon receiving {Esk (Mi), N2}, Ui, computes sk' = h (Bi ||Ni || Nj || y) and checks whether Dsk' (Esk (Mi)) = h (Bi Å Ni Å Nj Å y). It is obvious that the equality cannot hold since Ni is not equal to Ni*.

3.3 Server Spoofing Attack

In this proposed scheme, since the adversary can not construct the session key sk without the knowledge of Bi and y. After communicating with the masqueraded server, the legal user can detect immediately and terminate the session and therefore provides protection to the authorised user against the masqueraded threats.

3.4 Stolen Verifier Attack

As the verifier table is not a part of the proposed scheme it is an advantage in guarding the authentic user against stolen verifier attack.

3.5 Insider Attack

In the registration phase, instead of plain text, the password is submitted in the form of (PWi) the danger of revealing the password to S is eliminated thus threat against the insider attack is not completely elimininated.

3.6 User Anonymity Protected

The user Ui will send the login request {CIDi, Pi, Qi, N1} to the server in every login and even if the attacker intercepts and tries to analyse the login, message is infeasible to derive IDi from the login message due to the Phase 2 mentioned above. Further, as the login message is dynamic for each login and as the parameters of login message, CIDi is associated with nonce Ni and dynamically gets changed. Similarly, the values of Pi and Qi that are related to nonce Ni also get changed thus preventing the identity of the authentic user to the adversary.

3.7 Security of Session Key

The functions of the security session key provided in the proposed scheme are detailed in the following lines

3.7.1 Session Key Security

The session key is associated with Bi and y, which are unknown to the adversary and hence, the session key is known only to the user and the server.

3.7.2 Known Key Security

The session key is associated with Bi and y, which are unknown to the adversary. Even though the past session key sk is disclosed, the attacker cannot derive Bi and y based on the security of one-way hash function.

3.7.3 Forward Secrecy

By compromising the secret key x, the adversary can not compute Bi without PWi. Thus, the adversary can not derive the session key sk, since it is computed by h (Bi ||Ni || Nj || y).

4. FUNCTIONALITY AND PERFORMANCE ANALYSIS OF THE PROPOSED SCHEME

4.1 Functionality

The comparisons of functionality of the proposed scheme with that of other by considering the crucial criterions are presented in the Table 1.

Table1. Functionality comparisons among the proposed schemes and others

Criterions*	Proposed present	Chien, *et al.*	Juang	Das, *et al.*
C1	Not required	Not required	Not required	Not required
C2	Portable	Portable	Portable	Portable
C3	Low	Low	Low	Low
C4	Agrees	Agrees	Agrees	Not agrees
C5	Protects	Protects	Fails to protects	Fails to protects
C6	Exits	Not exits	Exits	Not exits
C7	Not exits	Exits	Exits	Exits

* C1: Verification table; C2: Freely chosen password; C3: Computation and communication cost; C4: Mutual authentication; C5: Session key agreement; C6: User's anonymity; C7: Time synchronisation problem.

Table 1 shows that the proposed scheme has improved functionality over other schemes and is more secured and reliable than other scheme owing to the user friendly time synchronisation compatibleness and protection of subsequent communication by the existence of session key agreement as well as protection to the users against threats like hackers, etc. due to the existence of user's anonymity.

4.2 Performance

The comparisons of dynamic ID-based present proposed scheme and other with respect to their performance based on computational cost are presented in the Table 2. The login phase of the proposed scheme is built with seven hash functions while Chien, *et al.* require each one symmetric key operation and exponentiation operation. Further, in the proposed scheme, in the authentication phase four symmetric key operations and eight hash functions have been incorporated in place of three symmetric key operations, three exponentiations and two hash functions in Chien, *et al.* scheme. Thus it can be concluded that the present proposed scheme offers lower computation costs.

5. CONCLUSION

The paper presented an efficient dynamic ID-based password authenticated key agreement scheme. The proposed scheme has the following advantages.

- The major intrinsic worth of this scheme include that, the system do not require any verification table and the user is at liberty to choose and change the password.
- Further, with this system, the computation and

Table2. Performance comparisons among the reposed schemes and others

Schemes	Computational cost of login phase	Computational cost of authentication phase
Present proposed	7H	4S+8H***
Chien, *et al.*	1S+1E	3S+3E+2H***
Juang	1S+1E+1H	3S+1E+2H***
Das, *et al*	5H	3H

communication costs are lower as the scheme adopts one-way hash functions, block ciphers and smartcard.

- In addition the scheme offers mutual authentication between server and user which is a nonce based plan that does not have any serious time-synchronization problem.
- The proposed system is secured against Id-theft, also resists to replay attacks, stolen verifier attacks, guessing attacks, reflection attack and offers forward secrecy and known-key security.

ACKNOWLEDGEMENTS

The authors are thankful to the management, principal and faculty of Don Bosco Institute of Technology, Bangalore, for the encouragement received throughout this research work.

REFERENCES

1. Lamport, L. Password authentication with insecure communication. *Communication ACM*, 1981, **24(**11), 770-72.

2. Awasthi, Amit.K. & Lal, Sunder. A remote user authentication with forward secrecy. *IEEE Trans. Consumer Electronics,* 2003, **49(**4), pp. 1246-48.

3. Chang, C. & Wu, T. Remote password authentication with smart cards. *IEEE Proceed.–Comp. Digital Techn.*, 1991, **138**(3), 165-68.

4. Chang, C. & Hwang, S. Using smart cards to authenticate remote passwords. *Compu. Mathe. Appli.* 1993, **26**(7), 19-27.

5. Chien, H.; Jan, J. & Tseng, Y. An efficient and practical solution to remote authentication: Smart card. *Computers and Security*, 2002, **21**(4), 372-75.

6. Chien, Hung-Yu & Chen, Che-Hao. A remote password authentication preserving user anonymity. *In* Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA '05), 2005.

7. Das, M.L.; Saxena, A. & Gulathi, V.P. A dynamic ID-based remote user authentication scheme. *IEEE Trans. Consumer Electron.*, 2004, **50**(2), 629-31.

8. Hwang, M.S. & Li, L.H. A new remote user authentication scheme using smart cards. *IEEE Trans. Consumer Electron.,* 2000, **46(1)**, 28-30.

9. Juang, W.; Lei, C. & Chang, C. Anonymous channel and authentication in wireless communications. *Computer Communications*, 1999, **22**(15-16), 1502-11.

10. Juang, W. Efficient password authenticated key agreement using smart cards. *Computers and Security*, 2004, **23**(2), 167-73.

11. Liao, I.; Lee, C.C. & Hwang, M.S. Security enhancement for a dynamic ID-based remote user authentication scheme. *In* Proceedings of the International Conference on Next Generation Web Services Practices (NWeSP'05), 2005.

12. Hwang, M.S. & Li, L.H. A new remote user authentication scheme using smart cards. *IEEE Trans. Consumer Electronic,* 2000, **46(**1), 28-30.

13. Wang, S.J. Yet another login authentication using N-dimensional construction based on circle property. *IEEE Trans. Consumer Electronic*, 2003, **49(**2), 337-41.

14. Lin, S. & Costello, D. Error control coding: fundamental and applications. Prentice–Hall, Englewood- Cliffs, NJ, 1983

15. Leveque, W. Elementary Theory of Number. Dover, 1990.

16. Shen, J.J.; Lin, C.W. & Hwang, M.S. A modified remote user authentication scheme using smart cards. *IEEE Trans. Consumer Electron.*, 2003, **49(**2), 414-16.

17. Leung, K.C.; Cheng, L.M.; Fong, A.S. & Chen, C.K. Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE Trans. Consumer Electron.*, 2003, **49(**3), 1243-45.

18. Lamport, L. Password authentication with insecure communication. *Communication of the ACM*, 1981, **24(**11), 770-72.

Invitation to Authors

If you are a library professional/information manager/information scientist/ information specialist/computer professional or a research scholar with a vision for developments in information technology, including software, processors, storage media, and devices having an impact on library and information systems and services, we invite you to submit a paper for *DESIDOC Journal of Library and Information Technology (DJLIT)* and enjoy the following benefits:

- Expert editorial support: All papers are wetted by the eminent members of the Editorial Board of *DJLIT.*
- Critical review: All papers are peer-reviewed by the experts in Library and Information Science.
- Extensive abstracting and indexing for greater visibility: *DJLIT* is covered in major indexing and abstracting services like *LISA and Indian Science Abstracts.* The full text of *DJLIT* is being reproduced in electronic databases of HW Wilson Company, namely, *OMNIFILE Full Text Select* and *OMNIFILE Full Text Mega* as well as *Indianjournals.com* and *Connectjournal.com.*
- Complimentary copies to the contributors.

Please send your paper/queries to:

The Editor(s)
DESIDOC Journal of Library & Information Technology
House Bulletin Group, 4th Floor
Defence Scientific Information & Documentation Centre
Defence Research & Development Organisation, Ministry of Defence
Metcalfe House, Delhi-110 054
e-mail:dbit@desidoc.drdo.in