International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.127-136
http://dx.doi.org/10.14257/ijsia.2014.8.6.12

An Improved Bilateral Remote User Authentication Scheme that Preserves User Anonymity using Symmetric Cryptology

Jung Gil Cho[1] and Won Whoi Huh[2]

*1 First Author *Division of Computer Engineering, SungKyul University, SungKyul University ro, Manan gu, Anyang si, Gyeonggi do, Republic of Korea (Zip code 430-742) jkcho@sungkyul.ac.kr*

*2 Corresponding Author *Division of Multimedia Engineering, SungKyul University, SungKyul University ro, Manan gu, Anyang si, Gyeonggi do, Republic of Korea(Zip code 430-742) wonwhoi@hanmail.net*

Abstract

In recent 2012, Wen and Li.'s has presented a dynamic ID-based remote user authentication with key agreement scheme. They claimed that their scheme can resisted insider attack and provide anonymity for the users. However, Juan Qu and Li-min Zou., described that Wen and Li.'s scheme could not withstand insider attack, does not provide anonymity for the users, and inefficiency for error password login. A different approach to symmetric cryptology is taken in this study to resolve the fore was made Compared to Juan Qu and Li-min Zou scheme, a different approach was made with symmetric cryptology in this study to supplement the forementioned weak points.

We propose an enhanced authentication scheme, which covers all the identified weakness of Wen and Li.'s scheme and an efficient user authentication scheme that preserve perfect anonymity to both the outsider and remote server.

Keywords: *bilateral authentication, smart card, symmetric cryptology, anonymity*

1. Introduction

Smart card authentication schemes have been widely deployed to verify the legitimacy of remote user's login request. Also, smart card is due to their low computation cost and convenient for the authentication purpose [1-9]. However, most of these schemes are based on static ID and have some flaws such as stolen, replay attack, insider attack, and impersonation attack, tracing attack. To overcome this vulnerability, Das, *et al.,* [10] proposed a dynamic ID-based remote user authentication scheme. But 2009 years, Wang, *et al.,* [11] showed that Das, *et al.,* scheme is completely insecure for its independence of using passwords, does not provide mutual authentication, and cannot resist forge server attack. Wang, *et al.,* proposed a dynamic ID-based remote user authentication scheme that a secure and efficient than the DAS scheme. In 2011, Khan, *et al.,* [12] and in 2013, K. C Shin [13] proposed an enhanced authentication scheme which covers all the identified weaknesses of Wang et al.'s scheme and is more secure and efficient for practical application environment. In 2012, Wen and Li's [14] proposed a dynamic ID-based authentication scheme with key agreement using symmetric cryptology which prevented security flaws and weaknesses of Wang, *et al.,* scheme [11]. Wen and Li's claimed that their scheme resisted impersonation attack and avoided the leakage of partial information. However, Kim, *et al.,* pointed out that Wen and Li's scheme leaked partial information concerning the communication party's secret

ISSN: 1738-9976 IJSIA

parameters and any adversary was able to exploit the leaked information to deduce session keys [15]. In 2013, Juan Qu and Li-min Zou, [16] described that Wen and Li's scheme could not withstand insider attack and forward secrecy, does not provide anonymity for the users, and inefficiency for error password login. To overcome the security flaws of Wen and Li's scheme, We propose an efficient user authentication scheme using secret key to generation of cipher text that preserve perfect anonymity to both the outsider and remote server.

2. Review of Wen and Li's Authentication Scheme

In this section, we briefly review Wen and Li's scheme [14], which consists of four basic parts namely, registration phase, login phase, authentication phase and key exchange phase, bilateral authentication and key confirmation phase. The following notations are used through this paper.

Table 1. Notation and Description

Ui	The ith user
IDi	The ith user's identity
pwi	The ith user's password
CIDi	The dynamic identity generated by the ith user
T	Timestamp
x	The server's secret number
SK	The session key
KC	The key confirmation message
$E_R[]/D_R[]$	Encode[]/Decode[] by symmetric key R

A. Registration Phase

(1) When a user Ui wants to register in the remote server, he/she sends his/her chosen IDi, pwi, to the remote server S via a secret channel.

(2) S computes ni= h(IDi‖pwi), where ni is the user's ID number and h(·) is a one way hash function. The unique number ni is kept by S to check the validity of the smart card, but the server does not need to keep the ID or password tables. Then S computes mi=ni⊕x, Ni=h(IDi)⊕h(pwi)⊕h(x)⊕h(mi), where x is the server's secret number kept by itself in private.

(3) S personalizes the smart card with the following parameters (h(·), Ni, ni).

(4) S sends the smart card to Ui via a secret channel.

B. Login Phase

When a user Ui wants to login S, then Ui inserts his/her smart card in the terminal and keys IDi and pwi, The smart card computes Ai=h(IDi)⊕h(pwi), Bi=Ni⊕h(IDi)⊕h(pwi)=h(x) ⊕h(mi), CIDi=h(Ai)⊕h(h(ni)⊕Bi⊕h(Ni)⊕T, and Ui forwards the login request message M1=(CIDi, ni, Ni, T) to the server S.

C. Authentication and Key Exchange Phase

Upon receiving the login request message M1=(CIDi, ni, Ni, T), S performs the following steps.

(1) Check if the time interval T'−T≤ ΔT, where T' is the current timestamp; if it holds and

ni is in the registered list, S continues the next step.

(2) S computes mi=ni⊕x, Bi=h(x)⊕h(mi), Ai=Ni⊕Bi=h(IDi)⊕h(pwi), and S checks whether the equation CIDi⊕h(Ai)=h(h(ni)⊕Bi⊕h(Ni)))⊕T holds.

(3) If so, S computes C'i =h(Ai⊕T'⊕h(ni)), and the session key SK =h(Ai‖T‖Bi‖T'), and key confirmation message KC'=h(Bi‖SK‖T').

(4) S sends the message M2 = (C'i, KC', T').

D. Mutual Authentication and Key Confirmation Phase

When Ui received M2 at time T", Ui performs the following steps.

(1) Check whether T' is valid.

(2) If the time interval is valid, Ui computes h(Ai⊕T⊕h(ni)) and verifies that the following equation holds: h(Ai⊕T'⊕h(ni)) =C'i.

(3) Ui computes SK =h(Ai‖T‖Bi‖T'), and then check if the equation h(Bi‖SK‖T') = KC' holds. If it holds, Ui computes KC =h(Ai‖SK ‖T").

(4) Ui sends the message M3 = (KC, T") to the server S.

(5) S verifies whether KC?=h(Ai‖SK ‖T") or not. If the equation holds, the scheme is over.

3. Security Weakness of Wen and Li's Scheme

In this section, Juan Qu and Li-min Zou [16] points out, Wen and Li's scheme looks at the vulnerability.

Juan Qu and Li-min Zou claimed that Wen and Li's scheme is vulnerable to insider attack, does not provide the user's anonymity, and is inefficient in error password login and when the private key of the server is compromised; the adversary can obtain all the previous session keys between the user Ui and the server S.

3.1 Weakness of Anonymity by Tracing

Anonymity refers to the act of a user using services or sources without having his identity exposed for once. For Wen and Li's Scheme, a user's identity is hardly exposed since M1=(CIDi, ni, Ni, T), one of the "login-request messages" is sent to the server.

However, we found that the user's anonymity of Wen and Li's scheme cannot be protected from an eavesdropping attack in the login phase.

The two "login-request" messages sent to the server, Ni=h(IDi)⊕h(pwi)⊕h(x)⊕h(mi) and ni=h(IDi‖pwi), can be perceived as the main reason in the erosion of anonymity. In other words, as long as a user's Ui pwi remains unchanged, the values of Ni and ni will be equal; then, the anonymity will eventually fade away with the tracking services implemented by attackers.

Therefore, Wen and Li's scheme fails in providing the privacy and anonymity of Ui during the login phase.

3.2. Privileged Insider Attack

In the registration phase of Wen and Li's scheme, when a user Ui wants to register in the remote server, he/she sends his/her chosen IDi, pwi, to the remote server S with plaintext via a secret channel. Then the Ui's password is possessed by the privileged insider.

An insider of the server can impersonate user's login by abusing the legitimate user's password and can get access to the other systems.

A lawfully-disguised-third-party knows Ui's password and thus not only can infer what "Ai" is from Ai=h(IDi)⊕h(pwi); but also "Bi" from "Bi=Ni⊕Ai". Based upon inferred

answers, a privileged insider can disguise as Ui to access another remote system by using "ni" and "Ni" and generate "CIDi(=h(Ai)⊕h(h(ni)⊕Bi⊕h(Ni)⊕T)".

That is, Wen and Li's scheme is vulnerable to insider attack.

3.3. Inefficiency for Error Password

In Wen and Li's Scheme, a supposition is made by a user's Ui that a password is entered with any errors. The calculation done by smart card is as follows.

Ai=h(IDi)⊕h(pwi)

Bi=Ni⊕h(IDi)⊕h(pwi)=h(x)⊕h(mi)

CIDi= h(Ai)⊕h(h(ni)⊕Bi⊕h(Ni)⊕T

The smart card still sends Ui's login request message M1=(CIDi, ni, Ni, T) unconditionally to server. Server S that received M1 will compute 2.3 of Authentication and Key Exchange Phase.

mi=ni⊕x

Bi=h(x)⊕h(mi)

Ai=Ni⊕Bi=h(IDi)⊕h(pwi)

and S checks whether the equation CIDi⊕h(Ai)=h(h(ni)⊕Bi⊕h(Ni)))⊕T

This error is not detected until the server checks CIDi⊕h(Ai)=?h(h(ni)⊕Bi⊕h(Ni)))⊕T at authentication phase.

This situation will waste unnecessary extra communication and computation cost. So, the password authentication is delayed and inefficient.

4. Description of the Proposed Authentication Scheme

This section introduces the proposed bilateral dynamic ID-based remote user authentication scheme using symmetric cryptology.

Improved idea is

· Defense against insider attack

· Ensure the anonymity with use symmetric cryptology

· Efficiency of the password verification

The proposed scheme is also divided into four phases, which are the user registration phase, the login phase, the authentication phase, and key confirmation phase. The details will be described as follows.

A. Registration Phase

(1) When a user Ui wants to register and become a legal user, Ui freely chooses his/her identity IDi and pwi, and submits IDi, h(IDi‖pwi) to the S via a secure communication channel.

(2) S computes

ni = h(IDi⊕x)⊕h(IDi‖pwi),

mi =ni⊕x,

Mi=h(IDi⊕x)⊕h(x),

Ni=h(x)⊕h(mi)⊕h(IDi‖pwi),

where x is the server's secret key kept in secretly.

(3) S stores (h(·), Ni, ni, Mi) in the smart card and submits the smart card to the Ui via a secure channel.

B. Login Phase

If Ui wants to access the server, he/she inserts smart card into the terminal, and keys IDi, with pwi, and smart card computes

$Bi=h(IDi\|pwi)\oplus Ni=h(x)\oplus h(mi)$

then the smart card verifies whether the equation $Ni=?Bi\oplus h(IDi\|pwi)$ holds or not.

If they are equal, the smart card accepts the login request and performs the following steps.

(1) The smart card chooses a random number r1 and computes

$Ai=h(r1\|pwi)$,

$CIDi =h(Ai)\oplus h(h(ni)\oplus Bi\oplus h(Ni)\oplus T)$,

$K=h(IDi\oplus x)\oplus r1$

$R=Mi\oplus r1=h(IDi\oplus x)\oplus h(x)\oplus r1$

(2) The smart card sends the login request message

$M1 = T, K, E_R[CIDi, Ni, ni, IDi]$ to the server S over a public channel.

C. Verification Phase

In this phase, when *S* receives the login request message from Ui, S performs the following steps.

(1) when S receives the login request message $M1 = T, K, E_R[CIDi, Ni, ni, IDi]$ at time T', the server S checks the validity of the timestamp T. If $T'-T\leq\Delta T$ holds and S moves on to the next step.

(2) S computes

$R=K\oplus h(x)=h(IDi\oplus x)\oplus r1\oplus h(x)$

Decode $E_R[CIDi, Ni, ni, IDi]$

$CIDi, Ni, ni = D_R[E_R[CIDi, Ni, ni, IDi]]$

$mi=ni\oplus x$

$Bi=h(x)\oplus h(mi)$

$Ai=Ni\oplus Bi=h(r1\|pwi)$

and verifies whether the equation $CIDi\oplus h(Ai)=?h(Bi\oplus h(Ni)\oplus h(ni)\oplus T)$ holds.

(3) If so, the server S computes the session key $SK=h(Ai\|T\|Bi\|T')$ and key confirmation message $KC'=h(Bi\|SK\|T')$. Then the server S submits the login response message $M2=T', E_R[KC', T']$ to the user Ui.

D. Bilateral Authentication and Key Confirmation Phase

In this phase, when Ui receives the login response message M2 from S, Ui performs the following steps.

(1) The user checks whether the timestamp is valid. If $T''-T'\leq\Delta T$ holds, the user Ui computes the session key $SK=h(Ai\|T\|Bi\|T')$ and key confirmation message $KC=h(Bi\|SK\|T')$ then verifies if KC is equal to KC'. If so, the user Ui computes the key confirmation message and $KC''=h(Ai\|SK\|T'')$ sends the message $M3=KC'', T''$ to the server S.

(2) When receiving the message M3 from the user Ui at time T^*. Check the validity of the time interval, if If $T^*-T''\leq\Delta T$ holds and the server S computes $KC'''=h(Ai\|SK\|T'')$ and verifies if KC''' is equal to KC''. If so, the message M3 is verified and the scheme is complete.

5. Security Analysis of the Proposed Scheme

This section describes the security analysis of the proposed scheme and compares performance with Wen and Li's scheme.

A. User Anonymity

User Ui anonymity is preserved at each login request. Ui compute to protect the user's anonymity and security of message, messages are transmitted after being encrypted using security information, R(=Mi⊕r1=h(IDi⊕x)⊕h(x)⊕r1). The E_R[CIDi, Ni, ni, IDi] is ciphertext of encrypted using secret key R. Suppose that an adversary intercepts the login request message M1 = T, K, E_R[CIDi, Ni, ni, IDi] in the login phase of our scheme; the user Ui has no way of guessing IDi because of the hardness of inverting of symmetric cryptology key R. Moreover, due to the random number r1, the user Ui cannot be traced out from the login request message M1. The value of K changes always since the random number "r1", especially, alters as each setting for sessions is configurated. Hence, in the presented scheme, an adversary cannot identify the person trying to login into the server. Our scheme is able to preserve the user's anonymity.

B. Insider Attack

In our proposed scheme, the user Ui freely chooses IDi, pwi and submits IDi, h(IDi‖pwi), to the S via a secure communication channel. So the insider of server S cannot compute the user's pwi from h(IDi‖pwi) because it is protected by hash function. Hence, Our scheme defends insider attack.

C. Bilateral Authentication and Session Key Agreement

In our proposed scheme, the user and the server can authenticate each other. The server verifies the legal user by verifying whether legitimately registered users should be able to generate "R(=Mi⊕r1)", the symmetric key.

Also the equation CIDi⊕h(Ai)=h(Bi⊕h(Ni)⊕h(ni)⊕T) holds.

Moreover, legitimate server S should be able to generate "R symmetric key" by using its own secret number x.

And the user can also verify the server by verifying whether KC=h(Bi‖SK‖T') and KC' are equal. The bilateral authentication protects against server side impersonation.

D. Replay Attack

The replay attacks cannot performance in proposed scheme. That is, replaying neither the login message [T, K, E_R[CIDi, Ni, ni, IDi] of login phase nor response message T', E_R[KC', T'] of authentication phase will not succeed since the encrypted message. Also, The login request message of our proposed protocol uses a random number r1(generate different every session) and timestamp to protect against replay attack. Since the attack is possible during the period of tolerant window ΔT in the time stamp based method, the proposed protocol applies the encryption scheme with session secrete key R.

Table 2. Comparison of Security Properties

	Wang, *et al.*,'s scheme [11]	Khan, *et al.*,'s scheme [12]	Wen, *et al.*,'s scheme [14]	Proposed scheme
Bilateral authentication	Yes	Yes	Yes	Yes
User anonymity	No	Yes	No	Yes
Insider attack	No	Yes	No	Yes
Impersonation attack	No	Yes	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes
Stolen attack	No	No	Yes	Yes
Key agreement	No	No	Yes	Yes
password error input check	No	No	No	Yes

Yes: supported and No: not supported.

E. Stolen Attack

If the user lost his smart card, the improved scheme still secures. It is presumed that "adversary" intercepts the messages M1, M2 and M3 sent between Ui and S, and can acquire the smart card's information Ni, ni and Mi. But does not know the user's password is the adversary, the adversary cannot derive Ai and Bi in our improved scheme. Additionally, M1 and M2 is codified by "R symmetric key"; M3 is a hash function value that it is impossible for adversary to figure it out. Thus the adversary A cannot calculate the session key SK=h(Ai‖T‖Bi‖T') and key confirmation message KC=h(Bi‖SK‖T'), which is a secret value between Ui and S. Therefore, the improved our scheme can resist the stolen attack.

F. Strengthening the Weak Point Caused by the Typographical Errors Made in Password

In Wen and Li's scheme, Ai, bi and CIDi are computed and sent to the server during the login stage. Server cannot decern the typographical errors made when entering passwords and will keep running until mi, Bi, and Ai are calculated, and (2) CIDi⊕h(Ai)=h(h(ni)⊕Bi⊕h(Ni)⊕T)) of 2.3 is compared.

However, in this study's scheme, before M1 is generated, the accuracy of password is checked first by computing "Bi" and Ni=?Bi⊕h(IDi‖pwi).

Likewise, by making up the weak point that rises due to typographical errors made when entering passwords, the problem of increase in a user's Ui and the server S is resolved.

6. Performance Comparison

In this section, we summarize the functionality comparisons between our scheme and other remote user authentication schemes in Table 2.

7. Conclusion

In this paper, we have presented cryptanalysis and weaknesses in Wen and Li.’s dynamic ID-based remote user authentication scheme, Firstly, We showed that Wen and Li.’s scheme is vulnerable to insider attack, does not preserved anonymity of a user, and no support for secret key generation during authentication process. To remedy these weaknesses and improve performance, we have proposed an enhanced remote user authentication scheme that

uses symmetric key cryptography (maintain anonymity), random number (prevent replay), an incorrect password check.

We have proposed a more completely and secure remote user authentication scheme preserving user anonymity. Which improves all the identified weakness of Wen and Li.'s scheme and is more secure. It is expected that the scheme proposed in this paper can be used in various applications for which smart cards are used.

References

[1] L. Lamport, "password authentication with insecure communication", communications of the ACM, vol. 24, no. 11, **(1981)**, pp. 770-772.
[2] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 1, **(2000)**, pp. 28-30.
[3] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocol", IEICE Transactions on communications E85-B, **(2002)** November, pp. 2519-2521.
[4] C. C. Lee, M. S. Hwang and W. P. Yang, "A Flexible Remote User Authentication Scheme using Smart Cards", ACM Operating System Review, vol. 36, no. 4, **(2002),** pp. 23-29.
[5] C. I. Fan, Y. C. Chan and Z. K. Zhang, "Robust remote authentication scheme with smart cards", Computers & Security, vol. 24, **(2005)**, pp. 619-628.
[6] I. E. Liao, C. C. Lee and M. S. Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme," KOREA: International Conference on Next Generation Web Services Practices, IEEE, **(2005).**
[7] N. Y. Lee and Y. C. Chiu, "Improved remote authentication scheme with smart card", Computer Standard & Interface, vol. 27, no. 2, **(2005),** pp. 177-180.
[8] Q. Xie, J.-K. Wang, D.-R. Chen and X.-Y. Wang, "A novel user authentication scheme using smart card", College of Computer Science. Zhejiang University. Hangzhou, 310027, P R China, and Graduate School, Hangzhou Normal University, **(2008)**.
[9] J. Xu, W. Zhu and D. Feng, "An improved smart card based password authentication scheme provable security", Computer Standard & Interface, vol. 31, **(2009),** pp. 723-728.
[10] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication Scheme", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, **(2004)** May, pp. 629-631.
[11] Y. Y. Wang, J. Y. Kiu, F. X. Xiao and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, vol. 32, **(2009)**, pp. 583-585.
[12] M. K. Khan, S. K. Kim and K. Alghathbar, "Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme", Computer Communications, vol. 34, **(2011)**, pp. 305-309.
[13] K. C. Shin, "A Robust and Secure Remote User Authentication Scheme Preserving User Anonymity", Society e-Business Studies (www.calsec.or.kr), (dx.doi.org/10.7838 /jsebs.2013.18.2.081), vol. 18, no. 2, **(2013)** May, pp. 81-93.
[14] F. Wen and X. Li, "An improved dynamic ID based remote user authentication scheme with key agreement scheme", Computers & Electrical Engineering, vol. 38, no. 2, **(2012)**, pp. 381–387.
[15] M. Kim, N. Park and D. Won, "Security weakness of a dynamic ID-based user authentication scheme with key agreement", CSA-12, LNEE, vol. 203, **(2012)**, pp. 687–692.
[16] J. Qu and L.-M. Zou, "An Improved Dynamic ID-Based Remote User Authentication with Key Agreement Scheme", Journal of Electrical and Computer Engineering, vol. 2013, Article ID 786587, pp. 5.

Authors

Jung Gil Cho, Division of Computer Engineering, Sungkyul University, #147-2, SungKyul University ro, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea, jkcho@sungkyul.ac.kr Education & Work experience: 2003, Ph.D. degree in dept. of Computer Engineering, Chungbuk National University. Currently: Professor in Division of Computer Engineering, Sungkyul University. Tel: 82-031-467-8916

Won Whoi Huh, Division of Multimedia Engineering, Sungkyul University, #147-2, SungKyul University ro, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea, wonwhoi@hanmail.net Education & Work experience: Graduate School of NID Fusion Technology, Digital Contents Design, 2012, Ph.D. Academic degree of Professional degree, IT & Design Fusion Program, Seoul national University of Science & Technology. Currently: Professor in Division of Multimedia Engineering, Sungkyul University. Tel: 82-031-467-8915.