An Improved Secure Dynamic ID-based Remote User Authentication Scheme with Key Agreement using Symmetric Cryptology

Mijin Kim[1], Junghyun Nam[2] and Dongho Won[1]

[1]*College of Information & Communication Engineering, Sungkyunkwan University, Korea*
[2]*Department of Computer Engineering, Konkuk University, Korea*
{mjkim, dhwon}@security.re.kr, jhnam@kku.ac.kr

Abstract

A dynamic ID-based user authentication scheme is designed to protect leakage of a user's partial information from intruders while enabling authenticated users to be granted access to the network service. In 2012, Wen and Li proposed a dynamic ID-based remote user authentication scheme with key agreement and claimed that their scheme resisted impersonation attacks and avoided leakage of partial information. However, Kim, et al., described that Wen and Li's scheme could leak some key information to an adversary and is vulnerable to a man-in-the-middle attack launched by any adversary. In this paper, we show how to solve the vulnerabilities in Wen and Li's scheme.

Keywords: *Security; authentication; key exchange; man-in-the-middle attack; stolen smart card attack*

1. Introduction

Current computing environments are full of interfaces via which humans must interact with computer systems. How to make those interfaces easy to use in a manner that results in secure interactions has always been a challenging problem.

A dynamic ID-based user authentication scheme is designed to protect leakage of a user's partial information from intruders while enabling authenticated users to gain access to customers, partners, and mobile employees securely [1, 2]. After Das, *et al.*, proposed a dynamic ID-based authentication scheme in 2004, researchers have proposed improved authentication protocols to eliminate the weaknesses in the previous authentication protocols [3-6]. In 2012, Wen and Li proposed a dynamic ID-based authentication scheme with key agreement using symmetric cryptology [7] which prevented security flaws and weaknesses of Wang, *et al.*'s scheme [6]. Session key was used to establish a secure communications channel in Wen and Li's scheme. A secure authentication with key agreement should accomplish both mutual authentication and session key establishment [8]. Wen and Li 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 parameters and any adversary was able to exploit the leaked information to deduce session keys [9]. In this paper, we propose an improved scheme to eliminate the security flaws of Wen and Li's scheme while maintaining the merits of the original scheme.

The rest of this paper is organized as follows. In Section 2, we review Wen and Li's scheme. In Section 3, the security weakness of Wen and Li's scheme is presented. In

Section 4, our improved dynamic ID-based remote user authentication scheme is proposed. The security analysis is described in Section 5. Finally, some concluding remarks are given in Section 6.

2. Wen and Li's scheme

Wen-Li's scheme consists of four basic phases: registration phase, login phase, authenticated key exchange phase, mutual authentication and key confirmation phase, and three functional phases: revocation phase, off-line password change phase and on-line secret renew phase.

The following notations are used through this paper.

Notation	*Description*
S	The service providing server
U_i	The ith user
ID_i	The ith user's identity
pw_i	The ith user's password
x	The server's secret number
A_i, B_i	The parameters for login
C_i	The parameter for ith user authentication
CID_i	The dynamic identity generated by the ith user
T	A timestamp
$\oplus$	The bitwise exclusive-or operator
$h(\cdot)$	A one-way hash function
$\|\|$	The concatenation operator
SK	The session key
KC	The key confirmation message

2.1. Registration phase

User U_i performs the registration phase to be a legal participant in the scheme. New users have to submit ID_i and pw_i to S through a secret channel. The detailed description is given below.

1. S computes $n_i = h(ID_i \| pw_i)$. The unique number n_i is kept by S to check the validity of the smart card.
2. S computes $m_i = n_i \oplus x, N_i = h(ID_i) \oplus h(pw_i) \oplus h(x) \oplus h(m_i),$ where x is $S's$ secret number.
3. S stores some parameters $h(\cdot), N_i,$ and n_i in the $U_i's$ smart card.
4. S sends the smart card to U_i through a secret channel.

2.2. Login phase

In this phase, when U_i wants to login the server S, U_i inserts his/her smart card and keys ID_i and pw_i. The smart card performs the following:

1. The smart card computes the needed parameters to create the login request message.
   $A_i = h(ID_i) \oplus h(pw_i), B_i = N_i \oplus h(ID_i) \oplus h(pw_i) = h(x) \oplus h(m_i), CID_i = h(A_i) \oplus h(h(n_i)$
   $\oplus B_i \oplus h(N_i) \oplus T).$
2. U_i sends the login request message $M_1 = \{CID_i, n_i, N_i, T\}$ to S.

2.3. Authentication and key exchange phase

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

1. Upon receiving the login request message at time T', S checks the validity of the timestamp T. If $T'-T \le \Delta T$ holds and n_i is in the registered list, S continues the next step.
2. S computes $m_i = n_i \oplus x, B_i = h(x) \oplus h(m_i), A_i = N_i \oplus B_i = h(ID_i) \oplus h(pw_i)$.
3. S verifies whether the equation $CID_i \oplus h(A_i) = h(B_i \oplus h(N_i) \oplus h(n_i) \oplus T)$ holds.
4. If so, S computes $C_i = h(A_i \oplus T' \oplus h(n_i))$. S can compute the session key $SK = h(A_i \| T \| B_i \| T')$, and key confirmation message $KC' = h(B_i \| SK \| T')$.
5. S sends the replied message $M_2 = \{C_i, KC', T'\}$.

2.4. Mutual authentication and key confirmation phase

In this phase, when U_i receives the replication at time T'', U_i performs the following steps.

1. U_i checks whether the timestamp T' is valid.
2. If the time interval is valid, U_i computes $h(A_i \oplus T' \oplus h(n_i))$ and verifies if it is equal to C_i.
3. U_i computes $SK = h(A_i \| T \| B_i \| T')$, then checks whether the key confirmation message KC' is correct. If so, U_i computes $KC = h(A_i \| SK \| T'')$.
4. U_i sends the message $M_2 = \{KC, T''\}$.
5. S verifies the message M_2, if the equation $KC = h(A_i \| SK \| T'')$ holds, this scheme is finished.

There are three additional functional phases: revocation phase, off-line password change phase, on-line secret renew phase in Wen-Li's scheme [7].

3. Security weaknesses of Wen and Li's scheme

We review the security weakness of Wen and Li's scheme described in [9]. In Wen and Li's scheme, when U_i sends the login request message M_1 to S through the public network, the secret values stored in U_i's smart card $\{N_i, n_i\}$ which is included in the message M_1 can be revealed. The adversary A may exploit these values to achieve an offline guessing attack and a man-in-the-middle attack.

3.1. Man-in-the-middle attack

We assume that the adversary A interposes the communication between U_i and S. A has intercepted the user U_i's login message $M_1 = \{CID_i, N_i, n_i, T\}$ and authentication and key exchange message $M_2 = \{C_i, KC', T'\}$ between U_i and S. Since the login request, and authentication and key exchange message are sent through the public network, any users including illegal ones can intercept them from the public network. Figure 1 shows the attack scenario where dashed line indicate that the corresponding messages are

intercepted by *A* en route its destination. A more detailed description of the attack is as follows:

1. From the intercepted message M_1 and M_2, the adversary *A* can obtain $h(n_i), T'$, and C_i. The leakage of this information is equivalent to compromise the secret A_i.

2. Therefore, the adversary *A* can calculate the session key $SK = h(A_i \| T \| B_i \| T')$ which is a secret value between U_i and *S*.

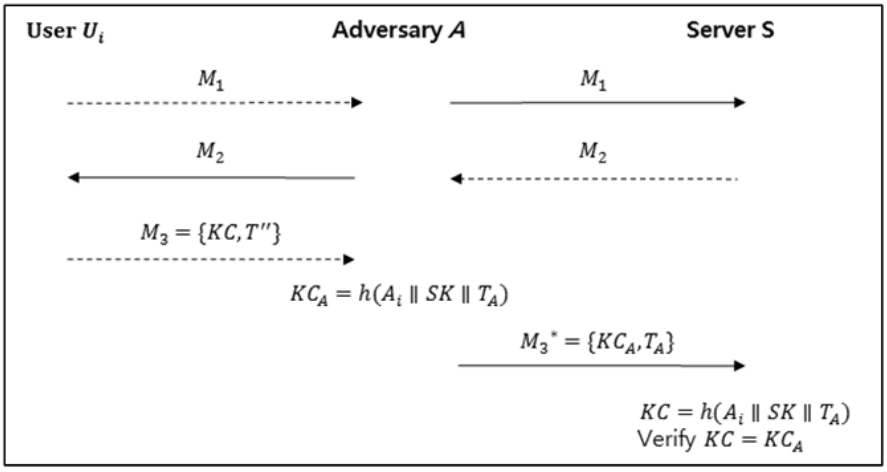

Figure 1. Man-in-the-middle attack on Wen-Li's scheme

3. Thereafter, *A* can impersonate *S* to U_i without knowing ID_i and PW_i.

4. On the other hand, upon receiving the message M_1 in Wen and Li's scheme, *S* computes and sends the replied message M_2 to U_i. However, this message is intercepted by the adversary *A*.

5. The adversary *A* forwards the message M_2 to U_i. Then U_i operates, as specified in Wen and Li's scheme, and sends the message $M_3 = \{KC, T''\}$ to *S*. However, this message is intercepted by *A* and creates a timestamp T_A, the adversary *A* computes $KC_A = h(A_i \| SK \| T_A)$, and *A* forges a message $M_3^* = \{KC_A, T_A\}$. Then, *A* sends the forged message M_3^*, as if it originated from U_i.

6. According to Wen and Li's scheme, upon receiving the message M_3^*, *S* verifies the last key confirmation message, whether the equation $KC = h(A_i \| SK \| T_A) = KC_A$ holds. Since M_3^* is valid, this passes, verifying U_i.

Following this, as described in the above attack, *S*, U_i, and adversary *A* share the session key *SK*. However, *S* and U_i cannot detect that they share the session key with the adversary *A*. From now, the adversary *A* could impersonate U_i to *S* and impersonate *S* to U_i, only through intercepting the message transmitted in the public channels. Such an attack could be serious, such as in the financial fields, where the adversary could impersonate the legal user

to transfer accounts to somebody. The worse effect could occur in the government or military departments [9].

4. Improved Scheme

In this section, we propose an efficient and secure scheme to avoid the security flaws of Wen and Li's scheme. Our scheme also involves the user (U_i) and the service providing server (*S*). The server chooses a master secret key *x*. There are four basic phases in our scheme: the registration phase, the login phase, the authentication and key exchange phase, and the mutual authentication and key confirmation phase. Figure 2 shows our improved remote user authentication scheme.

4.1. Registration phase

When the user U_i wants to access the services, he/she must submit his/her identity ID_i and password pw_i to *S* through a secure channel. The registration process proceeds as follows.

1. The user U_i chooses his/her identity ID_i and password pw_i, then submits ID_i and pw_i to the server *S* for registration via a secure channel. This secure channel ensures that the transmitted ID_i and pw_i in plaintext can be safe from the network attacks.
2. Upon receiving the message ID_i and pw_i, the server *S* computes $n_i = h(ID_i \| pw_i)$, $m_i = n_i \oplus x$, $N_i = h(ID_i) \oplus h(pw_i) \oplus h(x) \oplus h(m_i)$ for each user U_i. The unique number n_i is kept by *S* to check the validity of the smart card. *S* stores $(h(\cdot), N_i, n_i)$ in U_i's smart card and submits the smart card to the user U_i via a secure channel.

4.2. Login phase

When the user U_i intends to login to the server *S*, the user U_i inserts his smart card into a card reader and inputs his identity ID_i, password pw_i.

1. The smart card computes $A_i = h(ID_i) \oplus h(pw_i), B_i = N_i \oplus h(ID_i) \oplus h(pw_i) = h(x) \oplus h(m_i)$, $CID_i = h(A_i) \oplus h(h(n_i) \oplus B_i \oplus h(N_i) \oplus T)$ to create the login request message.
2. Then, the user U_i sends the login request message $M_1 = \{CID_i, n_i, N_i, T\}$ to the server *S* over a public channel.

4.3. Authentication and key exchange phase

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

1. when *S* receives the login request message at time T', the server *S* checks the validity of the timestamp *T*. If $T' - T \le \Delta T$ holds and n_i is in the registered list, *S* moves on to the next step.
2. *S* computes $m_i = n_i \oplus x$, $B_i = h(x) \oplus h(m_i)$, $A_i = N_i \oplus B_i = h(ID_i) \oplus h(pw_i)$, and verifies whether the equation $CID_i \oplus h(A_i) = h(B_i \oplus h(N_i) \oplus h(n_i) \oplus T)$ holds.

3. If so, the server S computes the session key $SK = h(A_i \| T \| B_i \| T')$, and key confirmation message $KC' = h(B_i \| SK \| T')$. Then the server S submits the login response message $M_2 = \{KC', T'\}$ to the user U_i.

4.4. Mutual authentication and key confirmation phase

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

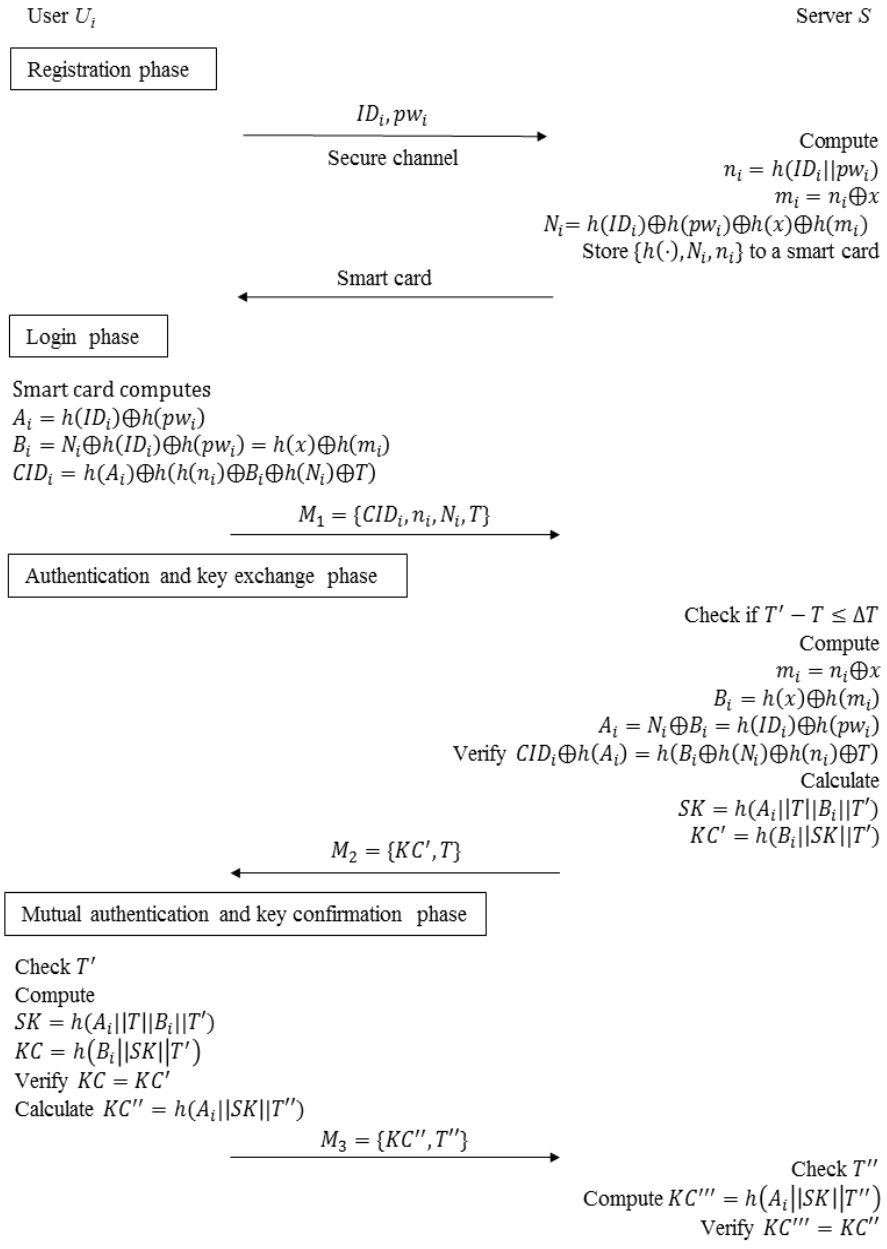

Figure 2. An improved remote user authentication scheme

1. The user U_i checks whether the timestamp T' is valid. If $T''-T' \leq \Delta T$ holds, the user U_i computes the session key $SK = h(A_i \| T \| B_i \| T')$, and key confirmation message $KC = h(B_i \| SK \| T')$, then verifies if KC is equal to KC'. If so, the user U_i computes the key confirmation message $KC'' = h(A_i \| SK \| T'')$ and sends the message $M_3 = \{KC'', T''\}$ to the server *S*.
2. When receiving the message M_3 from the user U_i the server *S* computes $KC''' = h(A_i \| SK \| T'')$, and verifies if KC''' is equal to KC''. If so, the message M_3 is verified and the scheme is complete.

There are three additional functional phases: revocation phase, off-line password change phase, and on-line secret renew phase described in Wen and Li's scheme [3].

5. Security Analysis

In this section, we analyze the security features of our improved scheme described in Section 4.

5.1. Man-in-the-middle attack

We assume that the adversary *A* interposes the communication between U_i and *S*. The adversary *A* has intercepted the user U_i's login message $M_1 = \{CID_i, N_i, n_i, T\}$ and authentication and key exchange message $M_2 = \{KC', T'\}$ between U_i and *S*. Since the login request, and authentication and key exchange message are sent through the public network, any users including illegal ones can intercept them from the public network. From the intercepted message M_1 and M_2, the adversary *A* cannot obtain A_i or B_i. In our improved scheme, the leakage of this information M_1 and M_2 is not useful to compromise the secret A_i or B_i. Thus, the adversary *A* cannot calculate the session key $SK = h(A_i \| T \| B_i \| T')$ which is a secret value between U_i and *S*. Therefore, the adversary *A* cannot impersonate *S* to U_i. On the other hand, upon receiving the message M_1 in our improved scheme, *S* computes and sends the replied message M_2 to U_i. Assume that the adversary *A* intercepts this replied message and forwards the message M_2 to U_i. Then, U_i proceeds as described in our scheme, and sends the message $M_3 = \{KC'', T''\}$ to *S*. Even if the adversary *A* intercepts the message M_3 and creates a timestamp T_A, the *A* cannot compute *SK* and impersonate U_i to *S*. In our improved scheme, even if an adversary or malicious user A has obtained the user U_i's login request message $M_1 = \{CID_i, n_i, N_i, T\}$, and authentication and key exchange message $M_2 = \{KC', T'\}$ between U_i and *S*, *A* cannot launch a man-in-the-middle attack. As previously described, our improved scheme is resistant to the man-in-the-middle attack.

5.2. Stolen smart card attack

Suppose an adversary has stolen U_i's smart card containing $(h(\cdot), N_i, n_i)$ and recorded the transmitted messages (M_1, M_2, M_3) between U_i and *S*. From the stolen smart card and intercepted messages, the adversary A cannot derive A_i or B_i in our improved scheme. The leakage of information $(h(\cdot), N_i, n_i, M_1, M_2, M_3)$ is not useful to compromise the secret A_i or B_i. Thus the adversary *A* cannot calculate the session key $SK = h(A_i \| T \| B_i \| T')$, which is a

secret value between U_i and *S*. Thus, the adversary *A* cannot perform the impersonation attack using the stolen smart card. Therefore, our improved scheme is secure against stolen smart card attacks. Table 1 compares security properties between our scheme and Wen and Li's scheme [7].

Table 1. Comparison of Wen-Li's scheme and our scheme

Security properties	*Wen-Li's scheme*	*Our scheme*
Anonymity	O	O
Man-in-the-middle attack	X	O
Stolen smart card attack	X	O
Mutual authentication	X	O

6. Conclusion

In 2012, Wen and Li proposed a dynamic ID-based remote user authentication scheme [7] with session key agreement and demonstrated its resistance to various attacks. However, Kim, *et al.*, described security weaknesses in the authentication and key exchange phase of Wen and Li's scheme and showed vulnerability to man-in-the-middle attack [9]. In this paper, we propose an improved scheme to solve the vulnerabilities in Wen and Li's scheme. The analyses show that our improved scheme remedies the weaknesses of Wen and Li's scheme.

Acknowledgements

This research was supported by the KCC (Korea Communications Commission), Korea, under the R&D program supervised by the KCA (Korea Communications Agency) (KCA-2012-12-912-06-003). Professor Dongho Won (dhwon@security. re.kr) is the corresponding author.

References

[1] W. Jeon, J. Kim, J. Nam, Y. Lee and D. Won, "An enhanced secure authentication scheme with anonymity for wireless environments", IEICE Transactions on Communications, vol. E95-B, no. 7, **(2012)**, pp. 2505-2508.
[2] J. Nam, S. Kim, S. Park and D. Won, "Security analysis of a nonce-based user authentication scheme using smart cards", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E90-A, no. 1, **(2007)**, pp. 299-302.
[3] M. L. Das, A. Saxana and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Transactions on Consumer Electronics , vol. 50, no. 2, **(2004)**, pp. 629-631.
[4] A. K. Awasthi, "Comments on a dynamic ID-based remote user authentication scheme", Transactions on Cryptology, vol. 1, no. 2, **(2004)**, pp. 15-16.
[5] W. C. Ku and S. T. Chang, "Impersonation attacks on a dynamic ID-based remote user authentication scheme using smart cards", IEICE Transactions, **(2005)**, pp. 2165-2167.
[6] Y. Y. Wang, J. Y. Liu, F. X. Xiao and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, vol. 32, no. 4, **(2009)**, pp. 583-585.
[7] 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.
[8] W. J. Tsaur, J. H. Li, and W. B. Lee, "An efficient and secure multi-server authentication scheme with key agreement", Journal of Systems and Software, vol. 85, no. 4, **(2012)**, pp. 876-882.
[9] 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.

Authors

Mijin Kim received her B.S., M.Ed degree in Mathematics Education from Sungkyunkwan University, Korea, in 1985 and 1989, respectively. She received her M.S. degree concentrated on Computing from Northeastern University, Boston, in 1997, and the Ph.D. degree in Electrical and Computer Engineering from Sungkyunkwan University, Korea, in 2011. She is now a research professor in Sungkyunkwan University, Korea. Her research interests include cryptography and information security.

Junghyun Nam received his B.E. degree in Information Engineering from Sungkyunkwan University, Korea, in 1997. He received his M.S. degree in Computer Science from University of Louisiana, Lafayette, in 2002, and the Ph.D. degree in Computer Engineering from Sungkyunkwan University, Korea, in 2006. He is now an associate professor in Konkuk University, Korea. His research interests include cryptography and computer security.

Dongho Won received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at ETRI (Electronics & Telecommunications Research Institute) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently Professor of School of Information and Communication Engineering. In the year 2002, he served as the President of KIISC (Korea Institute of Information Security & Cryptology). He was the Program Committee Chairman of the 8th International Conference on Information Security and Cryptology (ICISC 2005). His research interests are on cryptology and information security.