Enhanced Password-based Remote User Authentication Scheme Using Smart Cards[†]

Il-Soo Jeon[*] and Hyun-Sung Kim[**]

Abstract Secure and efficient authentication schemes over insecure networks have been a very important issue with the rapid development of networking technologies. Wang et al. proposed a remote user authentication scheme using smart cards. However, recently, Chen et al. pointed out that their scheme is vulnerable to the impersonation attack and the parallel session attack, and they proposed an enhanced authentication scheme. Chen et al. claimed that their scheme is secure against the various attacks. However, we have found that their scheme cannot resist the parallel attack and the stolen smart card attack. Therefore, in this paper, we show the security flaws in Chen et al.'s scheme and propose an improved remote user authentication scheme using tamper-resistant smart cards to solve the problem of Chen et al.'s scheme. We also analyze our scheme in terms of security and performance.

Key Words : Authentication scheme, Password-based, Smart card, Timestamp, Cryptography

1. Introduction

With the rapid development of various public networks, remote users can easily login and enjoy services on a server through the networks. Since the public networks are insecure, an authentication method is required for secure communications between the users and the server over the insecure networks. To authenticate each other, password-based authentication methods have been widely used. In 1981, Lamport [1] proposed an password-based remote user authentication scheme. However, the scheme is vulnerable to the server compromise attack and the verification table modification attack, because it has to maintain a verification table in the server. In order to overcome the problems, in 2000, Hwang and Li [2] proposed a remote user authentication scheme using smart cards based on ElGamal's public key cryptosystem, which does not use the verification table. Since then, many password-based authentication schemes using smart cards [3-17] have been developed. In order to enhance security and strong owner authentication of smart card, some research results using biometric information with smart cards [13-17] were published.

In 2000, Sun [3] proposed an efficient password based remote user authentication scheme using smart cards. Sun's scheme requires only several hash operations instead of the costly modular exponentiations. However, Sun's scheme does not provide mutual authentication. In 2002, Chien et al.

[†] This research was performed under the faculty's sabbatical year program of Kumoh National Institute of Technology.

[*] School of Electronic Engineering, Kumoh National Institute of Technology

[**] School of Computer Engineering, Kyungil University

[4] proposed an efficient remote user authentication scheme. But, in 2004, Ku-Chen [5] pointed out that Chien et al.'s scheme is vulnerable to the reflection attack, the insider attack, and is not repairable once the user's permanent secret is compromised, and they proposed an improved authentication scheme to resolve those security flaws in Chien et al.'s scheme. However, Yoon et al. [6] showed that Ku et al.'s scheme is susceptible to the parallel session attack and is insecure for changing the user's password, and they proposed an enhanced scheme of Ku et al.'s scheme. In 2007, Wang et al. [7] showed that both Ku et al.'s scheme and Yoon et al.'s scheme are vulnerable to the password guessing attack, the forgery attack, and the denial of service (DoS) attack. And they proposed an efficient improvement over Ku et al.'s and Yoon et al.'s schemes to overcome those flaws. However, recently, Chen et al. [8] pointed out that Wang et al.'s scheme is still vulnerable to the impersonation attack and the parallel session attack. To resolve those flaws in Wang et al.'s scheme, they proposed an improved scheme. We have found that Chen et al.'s scheme cannot resist the parallel attack.

In this paper, we show the security flaw in Chen et al.'s scheme and propose an improved password-based remote user authentication scheme using tamper-resistant smart cards. Most authentication schemes using smart cards including Chen et al.'s scheme are susceptible to stolen smart card attacks if not assuming that the smart cards have a tamper-resistant feature. Tamper-resistant technologies [18-22] have been developed with the various applications of smart cards.

The rest of this paper is organized as follows. In the following section, we review Chen et al.'s scheme, and cryptanalysis of their scheme. Then, we present an improved authentication scheme in Section 3. The security and performance analysis of the proposed scheme are discussed in Section 4. Finally, the conclusion is given in Section 5.

2. Review of Related Scheme and Cryptanalysis of it

In this section, we briefly discuss the attributes of smart cards that qualify them for remote user authentication schemes and review Chen et al.'s scheme [8] with the cryptanalysis of their scheme.

2.1 Attributes of Smart Cards

These days, smart cards play an important role in our everyday life. We utilize them as credit cards, electronic purses, health cards, and secure tokens for authentication of individual identity. But, since smart cards have low computing capability, lots of authentication schemes using smart cards have been designed without the public key cryptosystem technology for computation efficiency. Under the circumstances, if a smart card is lost or stolen, those schemes are inherently weak from the offline password guessing attack, because human-memorable passwords are not long enough to resist the attack.

Even if a smart card is lost or stolen, to protect important data in the smart card such as password and secret key information, proper tamper-resistant technologies in both hardware [18,19] and software [20,21] have been developed to counteract various attacks [22]. According to Smart Card Alliance, today's smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis [23].

It is important to develop authentication schemes using general smart cards, but it is usually insecure for the smart stolen attack. Considering the low computing capability of smart cards, authentication schemes using smart cards are required to have low computation cost by performing of hash functions or symmetric key cryptosystems as their main operations. Therefore, to develop an efficient and secure authentication scheme which can resist the smart card stolen attack, temper-resistant smart cards can be used.

<Table 1> Notations

Symbol	Description
U	The user
S	The remote server
ID	Identity of U
PW	Password of U
$h()$	Cryptographic un-keyed hash function
$h_p()$	Cryptographic keyed hash function including a secret code s
$E_K()/D_K()$	Symmetric key encryption /decryption with key K
x	Permanent secret key of S
T_u	Timestamp of U
T_s	Timestamp of S
SC	Smartcard
$\Rightarrow$	Sending message via a secure channel
$\rightarrow$	Sending message via a insecure channel
$\|$	Concatenation operator
$\oplus$	Exclusive-or operator

2.2 Chen et al.'s Scheme

In this section, we review Chen et al.'s scheme, which contains a registration phase, a login phase, a verification phase, and a password change phase. Each phase is described in the following subsections and illustrated briefly in Figure 1. To clearly describe Chen et al.'s scheme, some notations were used and summarized in Table 1. These notations will be also used in our scheme later.

2.2.1 Registration Phase

This phase is invoked whenever a user, U, initially registers or reregisters to the server, S. we briefly describe the phase in the following steps.

Step 1. U chooses a random number, b, and computes $h(b\oplus PW)$.

Step 2. $U \Rightarrow S$: $ID, h(b\oplus PW)$

Step 3. S performs the following computations: $P=h(ID\oplus x)$, $R=P\oplus h(b\oplus PW)$, $V=h_p(h(b\oplus PW))$, where x denotes Secret information maintained by S.

Step 4. $S \Rightarrow U$: The smart card containing $R, V, h()$, and $h_p()$.

Step 5. U enters b into his/her smart card. Now, U's smart card contains $b, R, V, h()$, and $h_p()$.

2.2.2 Login Phase

Whenever U wants to login S, the following steps will be performed.

Step 1. U inserts his smart card into the smart card reader, and then enters ID and PW.

Step 2. U's smart card computes $P=R\oplus h(b\oplus PW)$ and checks whether $V=h_p(h(b\oplus PW))$ holds or not. If not, the smart card terminates this session.

Step 3. U's smart card generates a random number, r, and computes $C_1=P\oplus h(r\oplus b)$, $C_2=h_p(h(r\oplus b)\parallel T_u)$, where T_u denotes U's current timestamp.

Step 4. $U \rightarrow S$: $\{ID, C_1, C_2, T_U\}$.

2.2.3 Verification Phase

After receiving the message, $\{ID, C_1, C_2, T_U\}$, S will perform authentication process with the smart card as following steps.

Step 1. S checks whether the format of ID is valid or not. If ID is not valid, S rejects the login request. Otherwise, S checks if both $T_u \neq T_s$ and $(T_s - T_u) < \Delta T$ hold or not, where T_s is the current timestamp of S and ΔT denotes the expected valid time interval for transmission delay. If they do not hold, S rejects U's login request.

Step 2. S computes $P = h(ID \oplus x)$, $C_1' = P \oplus C_1$, and $C_2' = h_p(C_1' \parallel T_u)$. Then, S checks if $C_2' = C_2$ holds or not. If it does not hold, S rejects U's login request. Otherwise, S authenticates U and accepts U's login request and computes $C_3 = h_p((C_1' \oplus T_s) \parallel P)$.

Step 3. $S \rightarrow U : \{T_s, C_3\}$

Step 4. Upon receiving the message, $\{T_s, C_3\}$, U checks if both $T_u \neq T_s$ and $(T_s - T_u) < \Delta T$ hold or not. If they do not hold, U terminates this session. Otherwise, U computes $C_3' = h_p(h(r \oplus b) \oplus T_s) \parallel P)$ and checks if $C_3' = C_3$ holds or not. If it does not hold, U terminates this session, otherwise U authenticates S.

U	S
Registration Phase $ID, h(b \oplus PW)$ →	
	$P = h(ID \oplus x)$ $R = P \oplus h(b \oplus PW)$ $V = h_p(h(b \oplus PW))$ $SC\ (R, V, h(), h_p())$ ←
Enter b into SC	
Login Phase Insert SC & Input ID, PW $P = R \oplus h(b \oplus PW)$ Verify $V = h_p(h(b \oplus PW))$ Generate random number r $C_1 = P \oplus h(r \oplus b)$ $C_2 = h_p(h(r \oplus b) \parallel T_u)$ ID, C_1, C_2, T_U →	
Verification Phase	Check validity of ID Verify $T_u \neq T_s$ & $(T_s - T_u) < \Delta T$ $P = h(ID \oplus x)$ $C_1' = P \oplus C_1$, $C_2' = h_p(C_1' \parallel T_u)$ Verify $C_2' = C_2$ $C_3 = h_p((C_1' \oplus T_s) \parallel P)$ T_s, C_3 ←
Verify $T_u \neq T_s$ & $(T_s - T_u) < \Delta T$ $C_3' = h_p(h(r \oplus b) \oplus T_s) \parallel P)$ Verify $C_3' = C_3$	
$SK = h(r \oplus b)$	$SK = C_1' = h(r \oplus b)$

<Figure 1> Chen et al.'s scheme

After successful authentication process, $C_1' = h(r \oplus b)$ shared between U and S can be used as the session key for the subsequent private communication.

2.2.4 Password Change Phase

This phase is invoked whenever U wants to change his/her password, PW, with a new one, PW_n.

Step 1. U inserts his smart card into the smart card reader, enters ID and PW, and requests to change password.

Step 2. U's smart card computes $P^* = R \oplus h(b \oplus PW)$ and $V^* = h_p^*(h(b \oplus PW))$.

Step 3. If V^* and V stored in smart card are equal, then U select new password PW_n, otherwise the smart card rejects the password change request.

Step 4. U's smart card compute $R_n = P^* \oplus h(b \oplus PW_n)$ and $V_n = h_p^*(h(b \oplus PW_n))$, and then replaces R, V with R_n, V_n, respectively. Now, the new password is successfully updated.

2.3 Cryptanalysis of Chen et al.'s Scheme

Chen et al. claimed that their scheme is secure against various attacks, but we have found that their scheme is vulnerable to the parallel attack. The parallel attack is performed by simply eavesdropping and sending the same login message of a legal user as soon as the legal user sends a login message to the server. It is a kind of the replay attack processing while the user's session is still open. Although their scheme is insecure for the password guessing attack if a smart card is lost or stolen, it can resist the attack by using a tamper-resistant smart card. Therefore, in this section, we only show the security weakness of their scheme for the parallel attack as following. While a user, U, sends a login message, $\{ID, C_1, C_2, T_u\}$, to the server, S, the attacker, E, eavesdrops the login message and sends the same message to S to request login. E's login message, $\{ID, C_1, C_2, T_u\}$, passes the validity test of ID and other verification on S. So, S authenticate E and responds to E with $\{T_s, C_3\}$, where $C_3 = h_p((C_1' \oplus T_s) \parallel P)$, $C_1' = h(r \oplus b)$. Therefore, E can masquerade as U and successfully be authenticated by S. Thus, Chen et al.'s scheme cannot resist this parallel attack.

3. Improved Authentication Scheme

In this section, we propose an enhanced remote user authentication scheme to overcome the weaknesses in Chen et al.'s scheme. Their scheme can resist the replay attack by using timestamps, but it cannot resist the parallel attack. To prevent our scheme from the parallel attack, we use the database of S to store the most recent session timestamp of U. And we use symmetric key cryptosystem to prevent an attacker, E, from modification or extraction of critical information in login and authentication messages. In addition, to resist the password guessing attack from the stolen smart card, we use tamper-resistant smart cards for our scheme. And our scheme is also able to provide a session key agreement after the authentication process.

The proposed scheme contains a registration phase, a login phase, a authentication phase, and a password change phase. Each phase is described in the following subsections and illustrated briefly in Figure 2.

3.1 Registration Phase

This phase is invoked whenever U initially registers or reregisters to S. We briefly describe the phase in the following steps.

Step 1. U chooses a random number, b, and computes $h(b \oplus PW)$.

Step 2. $U \Rightarrow S$: $ID, h(b \oplus PW)$

Step 3. S computes $R = h(ID \oplus x) \oplus h(b \oplus PW)$, where x denotes Secret information maintained by S.

Step 4. $S \Rightarrow U$: The smart card containing $(R, h(), E_K()/D_K())$.

Step 5. U enters b into his/her smart card. Then, U's smart card contains $(R, h(), E_K()/D_K(), b)$

3.2 Login Phase

Whenever U wants to login S, the following steps will be performed.

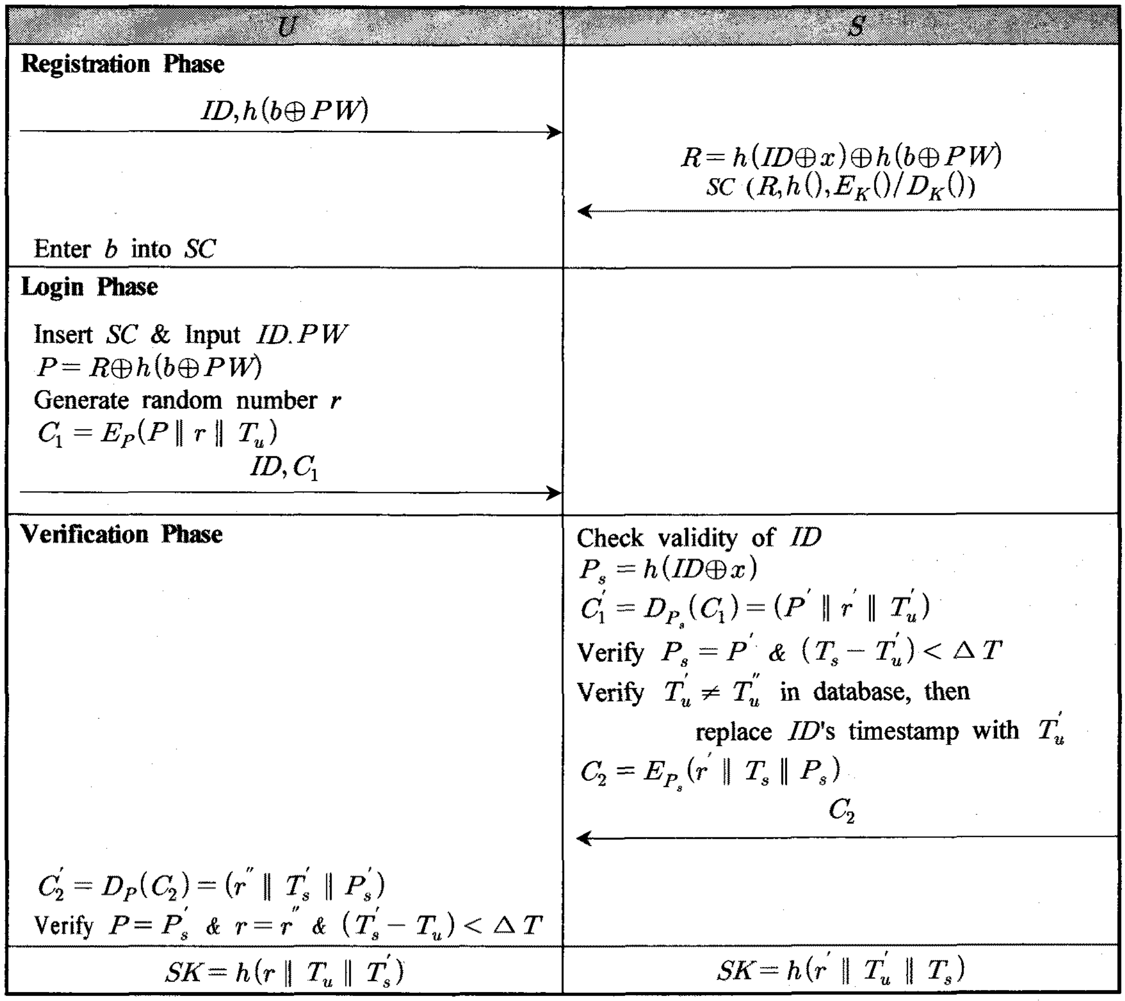
Step 1. U inserts his smart card into the smart card reader, and then enters ID and PW.

Step 2. U's smart card computes $P = R \oplus h(b \oplus PW)$, generates random number, r, and computes $C_1 = E_P(P \| r \| T_u)$, where $E_p()$ denotes encryption with key, P, and T_u denotes U's current timestamp.

Step 3. $U \rightarrow S$: $\{ID, C_1\}$

3.3 Verification Phase

After receiving the message, $\{ID, C_1\}$, S will



U	S
Registration Phase $ID, h(b \oplus PW)$ $\longrightarrow$	
	$R = h(ID \oplus x) \oplus h(b \oplus PW)$ $SC\ (R, h(), E_K()/D_K())$ $\longleftarrow$
Enter b into SC	
Login Phase Insert SC & Input $ID.PW$ $P = R \oplus h(b \oplus PW)$ Generate random number r $C_1 = E_P(P \| r \| T_u)$ ID, C_1 $\longrightarrow$	
Verification Phase	Check validity of ID $P_s = h(ID \oplus x)$ $C_1' = D_{P_s}(C_1) = (P' \| r' \| T_u')$ Verify $P_s = P'$ & $(T_s - T_u') < \Delta T$ Verify $T_u' \neq T_u''$ in database, then replace ID's timestamp with T_u' $C_2 = E_{P_s}(r' \| T_s \| P_s)$ C_2 $\longleftarrow$
$C_2' = D_P(C_2) = (r'' \| T_s' \| P_s')$ Verify $P = P_s'$ & $r = r''$ & $(T_s' - T_u) < \Delta T$	
$SK = h(r \| T_u \| T_s')$	$SK = h(r' \| T_u' \| T_s)$

<Figure 2> Proposed scheme

perform authentication process with the smart card in the following steps.

Step 1. S checks whether the format of ID is valid or not. If ID is not valid, S rejects the login request. Otherwise S computes $P_s = h(ID \oplus x)$ and $C_1' = D_{P_s}(C_1) = (P' \| r' \| T_u')$, where $D_{P_s}()$ denotes decryption with key, P_s.

Step 2. S checks if both $T' \neq T''$ and $(T_s - T_u') < \triangle T$ hold or not, where T_s is the current timestamp of S and $\triangle T$ denotes the expected valid time interval for transmission delay. If they do not hold, S rejects U's login request. Otherwise, S checks if $T_u' \neq T_u''$ hold or not, where T_u'' is the timestamp stored in the database at just previous session. If it does not hold, S rejects U's login request. Otherwise, S replaces T_u'' with T_u' and computes $C_2 = E_{P_s}(r' \| T_s \| P_s)$.

Step 3. $S \rightarrow U : \{C_2\}$

Step 4. Upon receiving the message, $\{C_2\}$, U decrypts C_2 with the key, P, to compute $C_2' = D_P(C_2) = (r'' \| T_s' \| P_s')$ and then checks if $P = P_s'$, $r = r''$, and $(T_s' - T_u) < \triangle T$ hold or not. If they do not hold, U terminates this session, otherwise, U authenticates S.

After successful authentication process, $h(r \| T_u \| T_s')$ on U and $h(r' \| T_u' \| T_s)$ on S can be used as the session key for the subsequent private communication.

3.4 Password Change Phase

The proposed scheme requires the server's help to change the password of users. We briefly describe the password changing process in the following steps.

Step 1: U performs the login and authentication process as described in Section 3.2 and Section 3.3. The inputted current password, PW, for login is maintained in the smart card until the completion of password changing process.

Step 2: After completing the login and authentication process successfully, U inputs a new password, PW_n, two times. If both of the inputted passwords are same, the smart card computes $R_n = R \oplus h(b \oplus PW) \oplus h(b \oplus PW_n)$ = $h(ID \oplus x) \oplus h(b \oplus PW_n)$. The user's password will be changed to the new password by replacing R with R_n on the smart card.

4. Security and Performance Analysis

In this section, we analyze the security of the proposed scheme by discussing its resistance to various attacks, and we discuss the performance of our scheme.

4.1 Security Analysis

In this section, we analyze the security of our scheme by showing its resistance to various attacks.

4.1.1 Impersonation Attack

It is difficult for an attacker, E, to successfully complete the impersonation attack on neither the user side nor the server side. For the user side, E cannot create a feasible $C_1 = E_P(P \| r \| T_u)$ without knowing the secret value, $P = h(ID \oplus x)$ which is used as the secret key of the encryption system. Since P is enclosed in $R = h(ID \oplus x) \oplus h(b \oplus PW)$ on U's smart card and the smart card has tamper-resistant feature, E cannot extract R and b. So, E cannot know the secret value, $P = h(ID \oplus x)$. Therefore, E cannot send a feasible login message to S as if he/she is U. For the server side, E cannot create a feasible $C_2 = E_{P_s}(r' \| T_s \| P_s)$ without knowing the secret value, $P_s = h(ID \oplus x)$ which is the secret key of the symmetric encryption system. Therefore, if E cannot send a feasible authentication message to U as if he/she is S. Thus, the proposed scheme is secure against the impersonation attack.

4.1.2 Replay Attack

To perform a replay attack, E will use a eavesdropped message, $C_1 = E_P(P \| r \| T_u)$, from one of the U's previous sessions which is not the last session. If E sends the eavesdropped message, C_1, to S, S will reject the login message by the verification of timestamp. Therefore, the proposed scheme is secure against the replay attack.

4.1.3 Parallel Attack

After U sends a login message, $C_1 = E_P(P \| r \| T_u)$, to S, assume that E also immediately sends the same message to S. However, E's message cannot pass the verification test, $T_u' \neq T_u''$, where T_u' is U's timestamp existing in decrypted message of C_1 and T_u'' is the most recent timestamp stored in database. In this verification of E's login message, T_u'' is the current session timestamp of U. Therefore, T_u' and T_u'' are equal and S rejects the E's login request. Thus, the proposed scheme is secure against the parallel attack.

4.1.4 Man-in-the-middle Attack

In the proposed scheme, login and authentication messages encrypted with the secret key, $P = h(ID \oplus x)$, cannot be released to E. Therefore, E cannot fabricate feasible messages in the middle of S and U. Therefore, the proposed scheme is secure against the man-in-the-middle attack.

4.1.5 Password Guessing Attack

It is difficult for E to guess the U's password based on the communication messages between S and U since the password is not included in them. Also, E cannot guess the password from the password table in S since the password table does not exist in S. Even if E gets the U's smart card, it is difficult for E to guess the U's password, because the password exists in the form of $h(ID \oplus x) \oplus h(b \oplus PW)$ in the smart card. To find the correct password, E has to able to guess the secret value, $h(ID \oplus x)$, and the random number, b. Because the smart card has a tamper-resistance feature, E cannot get the information from the smart card. So, E tries to guess $h(ID \oplus x)$ from the communication messages between S and U. But, $h(ID \oplus x)$ is always encrypted within the communication messages. Therefore, E cannot guess the password in our scheme. Thus, the proposed scheme is secure against the password guessing attack.

4.2 Performance Analysis

In this section, we evaluate the performance of our scheme in two aspects, security strength and the costs of computation and communication. To evaluate the performance, we compare our scheme to Chen et al.'s scheme. We showed the comparison results of computation and communication costs in Table 2.

We can say that the two schemes are efficient in computation because they do not use any modular exponentiations. Our scheme uses a symmetric key cryptosystem which is not used in Chen et al. It should be noted that the computational complexity of symmetric key encryption or decryption operation is similar to that of hash function operation.

<Table 2> Computation and communication costs comparison

Comparison factors	Chen et al.'s scheme	Our scheme
No. of hash op. in registration phase	5	3
No. of hash op. in login & authentication phase	11	2
No. of symmetric key encryption/decryption op.	0	4
No. of total hash & encryption/decryption op.	16	9
No. of insecure comm.	2	2

<Table 3> Security comparison

Comparison factors	Chen et al.'s scheme	Our scheme
Parallel attack resistance	No	Yes
Replay attack resistance	Yes	Yes
Man-in-the-middle attack resistance	Yes	Yes
No use of DB for message storing	Yes	No

Feldhofer and Rechberger [24] claimed that AES is even more efficient than SHA-256 in resource-constrained devices such as RFID tags. Therefore, it will not be a big problem even if we consider the symmetric key operation as the hash function operation to evaluate computation cost. Then, as shown in Table 2, the computation cost of our scheme is less than that of Chen et al.'s one. In communication cost, the two schemes both have 2 insecure communications.

In Table 3, we listed the comparison results about some security factors. As shown in Table 3, our scheme is more secure than Chen et al.'s scheme. Even if our scheme uses the database to store the user's timestamp, it is valuable because our scheme can resist the parallel attack by using it. Therefore, we can summarize that our scheme is more efficient and secure than Chen et al.'s scheme.

5. Conclusion

In this paper, we showed the vulnerability in Chen et al.'s password-based remote user authentication scheme, and proposed an enhanced password-based remote user authentication scheme based on tamper-resistant smart cards. We demonstrated that our scheme is efficient and secure against the various attacks through the analysis of security and computation costs. Therefore, considering the low computing capabilities of smart cards and the efficiency of our scheme, our scheme can be applied for practical uses.

References

[1] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, Vol. 24, No. 11, pp. 770 - 772, 1981.

[2] M.S. Hwang, L.H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28 - 30, 2000.

[3] H.M. Sun, "An efficient remote use authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, pp.958 - 961, 2000.

[4] H.Y. Chien, J.K. Jan, Y.M. Tseng, "An efficient and practical solution to remote authentication: smart card," Computers and Security, Vol.21, No. 4, pp. 372 - 375, 2002.

[5] W.C. Ku, S.M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 204 - 207, 2004.

[6] E.J. Yoon, E.K. Ryu, K.Y. Yoo, "Further improvement of an efficient password based

remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp. 612 - 614, 2004.

[7] X.M. Wang, W.F. Zhang, J.S. Zhang, M.K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," Computer Standards & Interfaces, Vol. 29, No. 5, pp. 507 - 512, 2007.

[8] T.H. Chen, H.C. Hsiang, W.K. Shih, "Security enhancement on an improvement on two remote user authentication schemes using smart cards," Future Generation Computer Systems, 2010 (in press).

[9] C.L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," Computers & Standards Interfaces, Vol. 26, No. 3, pp. 167 - 169, 2004.

[10] N.Y. Lee, Y.C. Chiu, "Improved remote authentication scheme with smart card," Computer Standards & Interfaces, Vol. 27, No. 2, pp. 177 - 180, 2005.

[11] J. Xu, W.T. Zhu, D.G. Feng, "An improved smart card based password authentication scheme with provable security," Computer Standards & Interfaces, Vol. 31, No. 4, pp. 723-728, 2009.

[12] R. Song, "Advanced smart card based password authentication scheme," Computer Standards & Interfaces, Vol. 32, No. 5, pp. 321-325, 2010.

[13] J.K. Lee, S.R. Ryu, K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," IEE Electronics Letters, Vol. 38, No. 12, pp. 554-555, 2002.

[14] H.S. Kim, S.W.Lee, K.Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," ACM Operating Systems Review, pp. 32-41, 2003.

[15] C.H. Lin, Y.Y. Lai, "A flexible biometrics remote user authentication scheme," Computer Standard & Interfaces, Vol. 27, No. 1, pp. 19-23, 2004.

[16] M.K. Khan, J. Zhang, "Improving the security of 'a flexible biometrics remote user authentication scheme," Computer Standards & Interfaces, Vol. 29, No. 1, pp. 82-85, 2007.

[17] C.T. Li, M.S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, Vol. 33, No. 1, pp. 1-5, 2010.

[18] O. Kommerling, M.G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," Proceedings of the USENIX Workshop on Smartcard Technology, pp. 9 - 20, 1999.

[19] S. Ravi, A. Raghunathan, S. Chakradhar, "Tamper Resistance Mechanisms for Secure Embedded Systems," IEEE Proceedings of the 17th International Conference on VLSI Design, pp. 605-611, 2004.

[20] H. Jin, G. Myles, J. Lotspiech, "Towards Better Software Tamper Resistance," Lecture Notes in Computer Science, Vol. 3650, pp. 417-430, 2005.

[21] P. Wang, S.K. Kang, K. Kim, "Tamper Resistant Software Through Dynamic Integrity Checking," The 2005 Symposium on Cryptography and Information Security, 2005.

[22] X. Leng, "Smart card applications and security," Information Security Technical Report, Vol. 14 pp. 36-45, 2009.

[23] http://www.smartcardalliance.org/pages/smart-cards-faq#how-do-smart-cards-help-to-protect-privacy

[24] M. Feldhofer, C. Rechberger, "A case against currently used hash functions in RFID protocols," Lecture Notes in Computer Science, Vol. 4277 pp. 372 - 381, 2006.

전 일 수 (Il-Soo Jeon)

- 1984년 경북대학교 전자공학과 공학사
- 1988년 경북대학교 전자공학과 공학석사
- 1995년 경북대학교 전자공학과 공학박사
- 1984년~1985년 삼성전자(주)
- 1989년~2004년 경일대학교 컴퓨터공학과 교수
- 2004년~현재 금오공과대학교 전자공학부 교수
- 관심분야 : 정보보호, 암호 프로토콜

김 현 성 (Hyun-Sung Kim)

- 1996년 2월 경일대학교 컴퓨터공학과 공학사
- 1998년 2월 경북대학교 컴퓨터공학과 공학석사
- 2002년 2월 경북대학교 컴퓨터공학과 공학박사
- 2002년 3월 ~ 현재 경일대학교 컴퓨터공학부 교수
- 관심분야 : 정보보호, 암호 프로토콜, 암호 프로세서 설계, IDS, PKI.

논문접수일 : 2010년 11월 22일
1차수정완료일 : 2011년 01월 03일
게재확정일 : 2011년 01월 05일