An Efficient and Secure Authentication Scheme Preserving User Anonymity*

Kim, Mi Jin · Lee, Kwang Woo · Kim, Seung Joo** · Won, Dong Ho***

〈Abstract〉

Authentication and key establishment are fundamental procedures to establish secure communications over public insecure network. A password-based scheme is common method to provide authentication. In 2008, Khan proposed an efficient password-based authentication scheme using smart cards to solve the problems inherent in Wu-Chieu's authentication scheme. As for security, Khan claimed that his scheme is secure and provides mutual authentication between legal users and a remote server. In this paper, we demonstrate Khan's scheme to be vulnerable to various attacks, i. e., password guessing attack, insider attack, reflection attack and forgery attack. Our study shows that Khan's scheme does not provide mutual authentication and is insecure for practical applications. This paper proposes an improved scheme to overcome these problems and to preserve user anonymity that is an issue in e-commerce applications.

Key Words : Mutual authentication, Reflection attack, Forgery attack, User anonymity

Ⅰ. Introduction

A password-based authentication scheme is commonly used to provide authentication between legal users and a remote server over public insecure networks. After Lamport[1] introduced a password-based remote authentication scheme, many researchers proposed the authentication schemes to improve security and efficiency, such as Encrypted Key Exchange(EKE)[2], Authenticated Key Exchange(AKE)[3] and Password-based Authenticated Key Exchange (PAKE)[4-5]. Although the construction and security analysis of password-based authentication schemes have a long history, they all have inherent weaknesses.

Smart cards have been widely adopted in many cryptographic protocols due to their low cost, portability and cryptographic capabilities. Password-based authentication schemes also used a smart card as a security token for more efficient execution.

* This work was supported in part by the Ministry of Knowledge Economy, Korea, under the Information Technology Research Center (ITRC) support program supervised by the National IT Industry Promotion Agency ((NIPA-2010-C1090-1001-0004), (NIPA-2010-C1090-1031-0005)) and in part by Priority Research Centers Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2010-0020210).
** Associate Professor, School of Information and Communication Engineering, Sungkyunkwan University
*** Professor, School of Information and Communication Engineering, Sungkyunkwan University (Corresponding author)

However, the resources in smart cards are constrained; the computation and the communication overhead must be low for practical implementation.

In 2004, Wu-Chieu[6] proposed a user friendly remote user authentication scheme with smart cards without requiring a user password table. In this scheme, users can choose and change their passwords freely. Furthermore, their scheme does not require the assignment of lengthy passwords. In 2008, Khan[7] showed that Wu-Chieu's scheme performs unilateral authentication (only client authentication) and there is no mutual authentication between the user and remote server. Thus, Wu-Chieu's scheme is vulnerable to server spoofing attack. Furthermore, their scheme is slow to detect the incorrect input-password, and users cannot change their passwords. Therefore, Khan[7] proposed an efficient and secure remote mutual authentication scheme, using one-way hash functions, to solve the problems found in Wu-Chieu's scheme.

In this paper, we demonstrate that Khan's scheme is vulnerable to various attacks, i. e., off-line password guessing attack, insider attack, reflection attack and forgery attack. Our study shows that Khan's scheme does not provide mutual authentication and is insecure for practical applications. This paper proposes an improved scheme to resolve these weaknesses and preserve user anonymity, a crucial issue in e-commerce applications.

The remainder of this paper is organized as follows: In Section Ⅱ, we review Khan's scheme and present our attacks on Khan's scheme. In Section Ⅲ, we demonstrate our proposed scheme. In Section Ⅳ, we analyze the security of our scheme. Finally, we conclude this work in Section Ⅴ.

Ⅱ. Review of Khan's Scheme

This section reviews Khan's scheme. Notation is provided. Then, the registration phase, the login phase, and the authentication phase of their scheme are described in turn. The password change phase is stated.

- ID_i : the identity of user U_i.
- PW_i : the password of U_i.
- h : a secure hash function.
- x : the permanent secret key of server S.
- y : the secret number of server S.
- $T, \Delta T$: the current timestamp and expected valid time interval for transmission delay, respectively.
- b, r_s: random numbers generated by U_i and S, respectively.
- E_k, D_k : symmetric encryption/decryption functions using symmetric key k satisfying $D_k(E_k(m)) = m$
- SK_u, SK_s: session keys generated by U_i and S, respectively. If the scheme ends successfully, then $SK_u = SK_s$.

Registration Phase The registration phase is invoked once when U_i initially registers to S, and is described, as follows:

1. U_i submits the registration request $< ID_i, PW_i >$ to S.
2. Upon receiving the registration request, S computes $A_i = h(ID_i \oplus x)$ and $V_i = A_i \oplus h(PW_i)$, then personalizes the smart card containing $< ID_i, A_i, V_i, h >$ and issues the smart card to U_i.

Login Phase When U_i wants to log into the system, U_i inserts the smart card into the card reader and enters ID_i and PW_i'. Then U_i's smart card computes $B_i = V_i \oplus h(PW_i')$, then verifies if B_i equals A_i. If they are equal, the smart card computes $C_1 = h(B_i \oplus T)$, otherwise terminates the operation. Finally, U_i sends the login message $< ID_i, C_1, T >$ to S over an insecure network.

Authentication Phase This phase is invoked when S receives U_i's login request, and described, as follows:

1. Upon receiving U_i's login request at time T', S checks the format of ID_i. If the format is incorrect, S rejects the login request. Then, S verifies the validity of time interval between T and T'. If $(T' - T) \geq \Delta T$, the S rejects the login request.
2. S computes $B_i' = h(ID_i \oplus x)$ and $C_1' = h(B_i' \oplus T)$, then checks if $C_1' ? = C_1$. If they are equal, U_i is authenticated and S accepts the login request. Otherwise, the login request is rejected. S acquires current timestamp T'' and computes $C_2 = h(B_i' \oplus T'')$ for mutual authentication message $< C_2, T'' >$ to U_i.

After receiving $< C_2, T'' >$ at time T''', U_i verifies the validity of the time interval between T'' and T'''. If the timestamp is invalid, U_i rejects further operations. U_i computes $C_2' = h(B_i \oplus T'')$ and compares $C_2' ? = C_2$. If they are equal, U_i believes that S is authenticated. Otherwise, U_i terminates the operation.

Password Change Phase When U_i wants to change the old password PW_i to new password PW_i^*, U_i inserts the smart card into a card reader, enters ID_i and PW_i', and requests the password change. The smart card then computes $B_i = V_i \oplus h(PW_i') = h(ID_i \oplus x)$, and then compares B_i and the stored value of A_i on the smart card. If they are equal, U_i is allowed to change the password. Otherwise, the password change request is rejected. Finally, the smart card computes $V_i' = B_i \oplus h(PW_i^*)$, and replaces V_i with V_i'.

2.1 Weaknesses of Khan's Scheme

In this section, we point out security weaknesses of Khan's scheme. These are shown through insider, reflection, password guessing, and forgery attacks, as well as other weaknesses of the scheme.

Insider Attack An insider attack is a malicious attack on a corporate system or network, where the adversary is someone who has been entrusted with authorized access to the network, and may have knowledge of the network architecture. In the registration phase of Khan's scheme, U_i's password is revealed to S. It is an insecure factor to submit plain PW_i to S. Leak of the password will be a threat to system security. If U_i used PW_i to access several servers for convenience, the insider of S may impersonate U_i to access other remote servers[8]. Thus, Khan's scheme cannot resist insider attack.

Reflection Attack A reflection attack is a method to attack a challenge-response authentication system that uses the same protocol in both directions. The essential idea of the attack is to trick the target into providing the answer to its own challenge.

In the login phase of Khan's scheme, if an adversary A intercepts and blocks the message

$< ID_i, C_1, T>$ transmitted in the login phase, A can impersonate S to send $< C_1, T>$ to U_i in the second step of authentication phase. Upon receiving the second item of the received message T, U_i computes $h(B_i \oplus T)$. Note that the second step of the authentication phase is skipped by A. U_i will be fooled into believing that the adversary is S, since the computed result equals the first item of the received message C_1.

Khan's scheme fails to provide mutual authentication, as claimed by the author, since U_i cannot authenticate S. Such a weakness may result in serious problems in some application systems[9, 10]. Therefore, in most real applications, one's private information should not be released to anyone until mutual confidence is established.

Password Guessing Attack A smart card is a memory card with an embedded micro-processor to perform the required operations specified by a scheme. No existing smart cards can prevent the information stored in them from being extracted, for example, by monitoring their power consumption[11, 12]. Some other reverse engineering techniques are also available to extract information from smart cards. Hence, we assume that once a smart card is stolen by an adversary A, all the information stored in it is known to A.

In Khan's scheme, suppose U_i's smart card is compromised by A, then A knows all the information $< ID_i, A_i, V_i, h >$ stored in the smart card. Thus, A can perform a password guessing attack to obtain PW_i by guessing a candidate password PW_i' and computing $A_i' = V_i \oplus h(PW_i')$. If the computed A_i' equals the stored A_i, this implies $PW_i' = PW_i$, A has successfully guessed U_i's password. Otherwise, A tries another candidate password. Therefore, Khan's scheme cannot resist password guessing attack.

Unlike typical private keys, a user's password has low entropy. The entropy of a user-generated password is about 2 bits per character[13]. Therefore, A can obtain a legitimate communication party's password within a reasonable time. Thus, password guessing attacks on the authentication schemes should be resisted.

Forgery Attack Since the adversary A may have $< ID_i, A_i, V_i, h >$ in the smart card, with this value, A can generate the forged login message $M = \{ID_i, C_A, T_A\}$, where $C_A = h(A_i \oplus T_A)$ and send this login message to S. Moreover, due to the unchangeableness of $A_i = h(ID_i \oplus x)$ in Kahn's scheme, a forged login request cannot be prohibited, even when U_i detected A_i has been compromised. Once A modifies C_1 to C_A and T to $T_A = (T_A - T) \geq \Delta T$, obviously the legal U_i's login request will be rejected by S due to T_A. Hence, Khan's scheme is vulnerable to forgery attack.

Other Weaknesses

1. We note that U_i's password is never used in the login and authentication phase of Khan's scheme, since $C_1 = A_i \oplus T$ and $C_2 = A_i \oplus T''$: it is only used by the smart card to verify whether the real holder or an imposter is using the smart card. Hence, it does not matter if U_i gives PW_i to S during the registration phase of Khan's scheme. Every insider who knows the secret x can impersonate everyone.
2. In Khan's scheme, when adversary A obtains

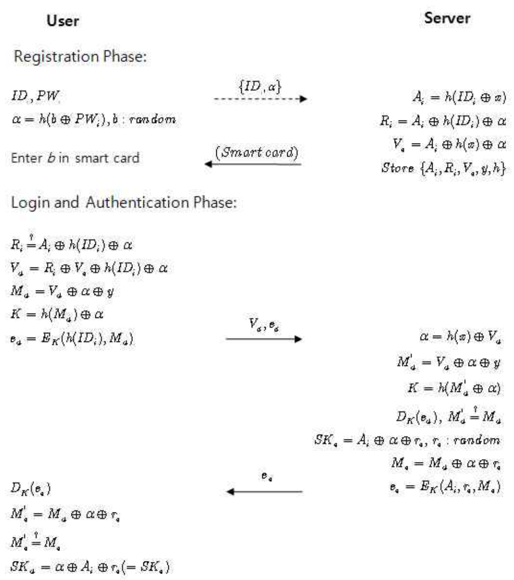
messages transmitted between U_i and S, A can know who communicates with S. This is undesirable. Recently, the authentication schemes are not only concerned about providing mutual authentication, but also in preserving user anonymity, because user privacy is an important issue in many e-commerce applications.

Ⅲ. Proposed Scheme

In this section, we propose an improved authentication scheme that resolves the security weaknesses described in the previous section. Our proposed scheme is efficient and more secure than Khan's scheme because there are only two messages exchanged for login/authentication and computations for hash function and symmetric encryption / decryption. Moreover, we establishes a session key K for use in securing their subsequent communications. The symmetric key K does not need to be exchanged during communication; U_i and S obtain K by computing it on each side. In our proposed scheme, U_i uses a secret number b which is not revealed to S. Additionally, our scheme provides the property of identity protection. <Figure 1> illustrates the scheme.

Registration Phase The registration phase is invoked once, when U_i initially registers to S, and is described, as follows:

1. U_i chooses ID_i and PW_i, generates a random number b, then computes $\alpha = h(b \oplus PW_i)$ and submits the registration request $< ID_i, \alpha >$ to S via a secure communication channel.



<Figure 1> Proposed Scheme

2. Upon receiving the registration request, S computes $A_i = h(ID_i \oplus x)$, $R_i = A_i \oplus h(ID_i) \oplus \alpha$ and $V_s = A_i \oplus h(x) \oplus \alpha$. Then, S stores the values $< A_i, R_i, V_s, y, h >$ in a smart card and issues the smart card to U_i.
3. U_i enters b into the smart card, then U_i's smart card contains $< A_i, R_i, V_s, y, h, b >$. From henceforth, U_i does not need to remember b.

Login Phase This phase is invoked whenever U_i intends to login S. U_i connects his smart card to a reader. The smart card challenges U_i for ID_i and PW_i. These are selected at U_i's application. Then the smart card computes $\alpha = h(b \oplus PW_i)$ and checks $R_i = A_i \oplus h(ID_i) \oplus \alpha$.

Next, U_i computes $V_u = R_i \oplus V_s \oplus h(ID_i) \oplus \alpha$, $M_u = V_u \oplus \alpha \oplus y$, $K = h(M_u) \oplus \alpha$. Then, U_i encrypts ID_i and M_u using K, yielding $e_u = E_K(h(ID_i), M_u)$. Finally,

U_i sends V_u and e_u to S.

Authentication Phase This phase is invoked when S receives U_i's login request, and is described, as follows:

1. Upon receiving U_i's login request, S obtains $\alpha = h(x) \oplus V_u$ and computes $M_u' = V_u \oplus \alpha \oplus y$, $K = h(M_u') \oplus \alpha$. After decrypting $D_K(e_u)$, S verifies $M_u' ? = M_u$. If $M_u' = M_u$, then U_i is authenticated and accepts the login request. Otherwise, S disconnects the connection. Then, S randomly creates a nonce r_s and computes $SK_s = A_i \oplus \alpha \oplus r_s$, $M_s = M_u \oplus \alpha \oplus r_s$. Next, S encrypts A_i, r_s and M_s using K, yielding $e_s = E_K(A_i, r_s, M_s)$. Finally, S sends e_s to U_i.
2. After receiving e_s and decrypting $D_K(e_s)$, U_i computes $M_s' = M_u \oplus \alpha \oplus r_s$ and verifies $M_s' = M_s$. If $M_s' = M_s$, S is authenticated. Otherwise, U_i disconnects the connection. Then, U_i computes $SK_u = \alpha \oplus A_i \oplus r_s$, which is equal to SK_s.

The password update phase When U_i intends to change password, U_i inserts his smart card into a reader, announces a password update request at U_i's terminal and keys PW_i. Then, the smart card calculates $h(b \oplus PW_i)$ and U_i gives a new password PW_i^*. Next, the smart card calculates $V_s' = V_s \oplus \alpha \oplus h(b \oplus PW_i^*)$ and $R_i' = R_i \oplus \alpha \oplus h(b \oplus PW_i^*)$. Finally, U_i replaces $< V_s, R_i >$ with this new $< V_s', R_i' >$.

Ⅳ. Security Analysis

In this section, we briefly demonstrate that our proposed scheme is secure against an insider attack, a reflection attack, a password guessing attack, a forgery attack and a stolen smart card attack.

1. Resistance to insider attack. Since U_i registers to S by presenting $\alpha = h(b \oplus PW_i)$ instead of PW_i, the insider S cannot directly obtain PW_i. Furthermore, as b is not revealed to S, the insider of S cannot obtain PW_i by performing a password guessing attack on α. Therefore, the proposed scheme can resist the insider attack.
2. Resistance to reflection attack. An adversary A may intercept or eavesdrop communication between U_i and S. After intercepting the message $< V_u, e_u >$ sent by U_i, A may impersonate and replay the message to S. Even if A has the response message e_s from S, A cannot extract values in e_s without knowing K, which is never exposed on the communication. In addition, A cannot forge a message to impersonate U_i or S without knowing K. Our proposed scheme uses symmetric key K to prevent the reflection attack, described in Section 2. Moreover, K does not need to be exchanged during communication; U_i and S can obtain K by computing it on each side. Thus, the proposed scheme can withstand reflection attack.
3. Resistance to password guessing attack. Suppose adversary A knows all the values $< A_i, V_s, R_i, y, b, h >$ in U_i's smart card and intercepts $< V_u, e_u, e_s >$ transmitted between U_i and S. Even if A uses all the intercepted messages and extracted values in U_i's smart card, the password guessing attack is impossible, because A cannot obtain K without knowing α. Therefore, the proposed scheme is secure against password guessing attack, described in Section 2.

4. Resistance to forgery attack. An adversary A may attempt to modify U_i's login message $< V_u, e_u >$ into $< V_u^*, e_u^* >$. However, this impersonation attempt fails, because A has no way to obtain the values $(h(ID_i), \alpha)$ to compute the valid login message. Therefore, the proposed scheme can resist the forgery attack, described in Section 2.
5. Resistance to stolen smart card attack. Suppose A has stolen U_i's smart card and recorded the transmitted messages (V_u, e_u, e_s) during one of U_i's past sessions. However, since A does not know ID_i and PW_i, A cannot forge the message between U_i and S that passes login verification or forge SK_u and SK_s without knowing PW_i and r_s. Therefore, the proposed scheme can withstand the stolen smart card attack.

<Table 1> Efficiency and Functionality comparison of related scheme

	Proposed Scheme	Khan's Scheme	Wu-Chieu's Scheme
F1	$3T_h$	$2T_h$	$1T_{\exp}, 2T_h$
F2	$2T_h, 1T_{enc}$	$2T_h$	$1T_{\exp}, 2T_h$
F3	$2T_h, 1T_{enc}, 1T_{dec}$	$4T_h$	$1T_{\exp}, 2T_h$
F4	Yes	Yes?	Yes?
F5	Yes	Yes	No
F6	Yes	No	No
F7	Yes	No	No
F8	Yes	Yes	No

F1: Computation in Registration Phase,
F2: Computation in Login Phase
F3: Computation in Authentication Phase
F4: Mutual Authentication
F5: Freely Changed Password
F6: Session Key Agreement
F7: User Anonymity
F8: Fast Incorrect Password Detection
T_h: the computation time for a hash function
$T_{\exp}$: the computation time for modular exponentiation
T_{enc}/T_{dec}: the computation time for symmetric encryption/decryption
?: Authors claimed yes but failed

<Table 1> summarizes the efficiency and functionality comparison between our proposed scheme and related schemes.

Ⅴ. Conclusion

In 2008, Khan proposed a remote mutual authentication scheme using smart cards and demonstrated its resistance to various attacks. However, after reviewing Khan's scheme and analyzing its security, various attacks, i. e., password guessing attack, insider attack, reflection attack and forgery attack, are presented in different scenarios. The analyses show that the scheme does not provide mutual authentication and is insecure for practical applications. We propose an improved scheme preserving user anonymity. It improves resistance to the password guessing attack, insider attack, reflection attack, forgery attack and stolen smart card attack to avoid these attacks.

References

[1] Lamport, L., "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24, No. 11, 1981, pp. 770-772.
[2] Bellovin, S. M. and Merritt, M., "Encrypted key exchange: password-based protocols secure against dictionary attacks," In: IEEE Symposium on research in security and privacy, IEEE Computer Society, 1992, pp. 72-84.
[3] Bellare, M., Pointcheval, D. and Rogaway, P., "Authenticated key exchange secure against dictionary attacks," Advances in Cryptology-

EUROCRYPT00, Lecture Notes in Computer Science, 1807, 2000, pp. 139-155.

[4] Botko, V., Mackenzie, P. and Patel, S., "Provable secure password-authenticated key exchange using Diffe-Hellman," 2000, pp. 156-171.

[5] Yang, G., Wong, D. S., Wong, H. and Deng, X., "Two-factor mutual authentication based on smart cards and passwords," Journal of computer and system sciences, Elsevier, Vol. 74, No. 7, 2008, pp. 1160-1172.

[6] Wu, S. T. and Chieu, B. C., "A note on a user friendly remote user authentication scheme with smart cards," IEICE Transactions Fundamentals, Vol. 87-A, No. 8, 2004, pp. 2180-2181.

[7] Khan, M. K., "An efficient and secure remote mutual authentication scheme with smart cards," International Symposium on Biometrics and Security Technologies(ISBAST 2008), pp. 1-6.

[8] Ku, W. C., Chen, C. M. and Lee, H. L., "Cryptanalysis of a variant of Peyravian-Zunic's password authentication scheme," IEICE trans. on commun., Vol. E86-B, No. 5, 2003, pp. 1682-1684.

[9] Mitchell, C., "Limitations of challenge-response entity authentication," Electronics Letters, Vol. 25, No. 17, 1989, pp. 1195-1196.

[10] Yashinsac, A., "Dynamic analysis of security protocols," Proc. 2000 Workshop on New Security Paradigms, 2001, pp. 77-87.

[11] Kocher, P., Jaffe, J. and June, B., "Differential power analysis," Proc. Advances in Cryptology (CRYPTO'99), 1999, pp. 388-397.

[12] Messerges, T. S., Dabbish, E. A. and Sloan, R. H., "Examming smart card security under the threat of power analysis attacks," IEEE Transactions on Computer, Vol. 51, No. 5, 2002, pp. 541-552.

[13] Menezes, A. J., Oorschot, P. C. and Vanston, S. A., "Handbook of applied cryptography," CRC Press, New York, 1997.

■ Authors ■

Kim, Mi Jin

Sep. 2006~Current
Ph. D. candidate of the School of Information and Communication Engineering from Sungkyunkwan University, Korea
Jun. 1997 M. S. degree from Northeastern University, Boston, USA
1985, 1989 B. S. M. Ed. degrees from Sungkyunkwan University, Korea

Interest : Cryptographic protocols, information security and network security
E-mail : mjkim@security.re.kr

Lee, Kwang Woo

Feb. 2007~Current
Ph. D. candidate of the School of Information and Communication Engineering from Sungkyunkwan University, Korea
2005, 2007 B. S. and M. S. degrees in Computer Engineering from Sungkyunkwan University, Korea

Interest : Cryptography, information security and information assurance, e-voting
E-mail : kwlee@security.re.kr

Kim, Seung Joo

Mar. 2004~Current
Professor of School of Information and Communication Engineering of Sungkyunkwan University, Korea
1994, 1996, 1999
B. S., M. S., and Ph. D. degrees in Information Engineering from Sungkyunkwan University, Korea

Interest : Cryptography, information security and information assurance
E-mail : skim@security.re.kr

Won, Dong Ho

Mar. 1982~Current
Professor of School of Information and Communication Engineering of Sungkyunkwan University, Korea
1976, 1978, 1988
B. S., M. S., and Ph. D. degrees in Electronic Engineering from Sungkyunkwan University, Korea

Interest : Cryptology and information security
E-mail : dhwon@security.re.kr

Received 19 August 2010
Received in revised form 25 August 2010
Accepted 30 August 2010