Cryptanalysis on Improved Remote User Authentication Scheme Preserving User Anonymity

Sung-Woon Lee, **Hyuck-Jin Kwon,** **and Hyun-Sung Kim***

Tongmyong Univ., Korea Tongmyong Univ., Korea Kyungil Univ., Korea

Summary
Even though user anonymity is an important issue in many e-commerce applications, most of smartcard-based remote authentication schemes did not considered user identities protection while authenticating the users. In 2004, Das et al. proposed a remote authentication scheme by preserving the users' anonymity. Their scheme adopted dynamic identification to achieve the property. In 2005, Chien and Chen pointed out that Das et al.'s scheme fails to protect the user's anonymity, and enhanced the scheme. However, Hu et al. in 2007 showed that their scheme also has some problems including masquerading attacks, insider attack, and replay attack and presented an improved scheme to conquer these problems. This paper shows that Hu et al.'s scheme still suffers from some attacks. The scheme could not only suffer from strong user/server masquerading attacks and denial of service attack but also not support the user anonymity. Additionally, this paper points out that the method to prevent the insider attack in the scheme is not applicable in reality.

Key words:
Authentication, Password-based Authentication, Smartcard, User Anonymity.

1. Introduction

Remote user authentication using smartcards is the most widely used scheme for a valid user to login to a remote server and to access the services provided by the server over insecure channels. Due to the convenience, secure storage, and secure computation of smartcards, many smartcard-based remote authentication schemes have been proposed [7-10]. Most of these schemes have the following good properties: (1) the server has no password table; (2) users can freely choose their own passwords; (3) it demands only low communication and computation cost; (4) mutual authentication is provided between a user and a server.

However, these schemes did not protect the users' identities, even though user anonymity is an important issue in many e-commerce applications. In 2004, Das et al. proposed a smartcard-based user authentication scheme by adapting a dynamic identification being changed in each user's login request to achieve the user anonymity [1]. Chien and Chen in 2005 showed that Das et al.'s scheme does not protect the user anonymity and proposed an improved scheme with generating a session key [2]. However, Hu et al. pointed out that Chien and Chen's scheme also has some problems [3]: it cannot resist strong server/user masquerading attack, insider attack [4], denial of service attack and restricted replay attack [5]; it has the problem of slow wrong password detection [6]. So they proposed an improved scheme to solve these problems. Counter in the scheme is adopted instead of using timestamps, i.e. system-widely synchronized clocks, so that the recipients can verify the timeliness of the messages and reject replaying messages used in the past sessions.

Unfortunately, this paper describes that Hu et al.'s scheme is still vulnerable to strong server/user masquerading attack and denial of service attack and does not provide user anonymity. Furthermore, the scheme requires that the user should store a random number in its own smartcard after being issued the smartcard from the server in the user registration phase to prevent the insider attack. Additionally, we points out that this is not applicable in reality.

This paper is organized as follows. Section 2 gives a review of Hu et al.'s scheme. Some cryptanalysis of the scheme are presented in section 3. Finally, section 4 gives a brief conclusion.

2. Review of Hu et al.'s Scheme

In this section, we will first describe the notations being used in this paper and review Hu et al.'s authentication scheme in detail. Table 1 presents the notations used in Hu et al.'s scheme. Hu et al.'s scheme was proposed to solve

* Corresponding author

Manuscript received October 5, 2008
Manuscript revised October 20, 2008

the problems in Chien and Chen's scheme: it cannot resist strong server/user masquerading attack, insider attack, denial of service attack and restricted replay attack; it has the problem of slow wrong password detection. The scheme adapted counters instead of using timestamps to prevent the denial of service attack and the restricted replay attack. Also to resist the insider attack in the scheme which is common in most of smartcard-based remote authentication schemes, the scheme employed one method by adopting random number so that the manager of the remote server can obtain no information about the user's password in the registration phase.

Table 1: Notations

Symbol	Description
U	the user
S	the remote server
ID	the identity of U
pw	the password of U
a, b, t, e	random numbers
x	the strong secret key of S
$h()$	a secure one-way hash function
p, q	the parameters for Diffie-Hellman Key exchange protocol
N_U, N_S	the counters of U and S, respectively
$\oplus$	the exclusive-OR (XOR) operation
$E_k[X]$	encrypting X using symmetric key k
- - - -▶	secure channel transfer
——▶	insecure channel transfer

Hu et al.'s scheme is composed of the registration phase, the login phase and the authentication phase. The scheme performs as Fig. 1.

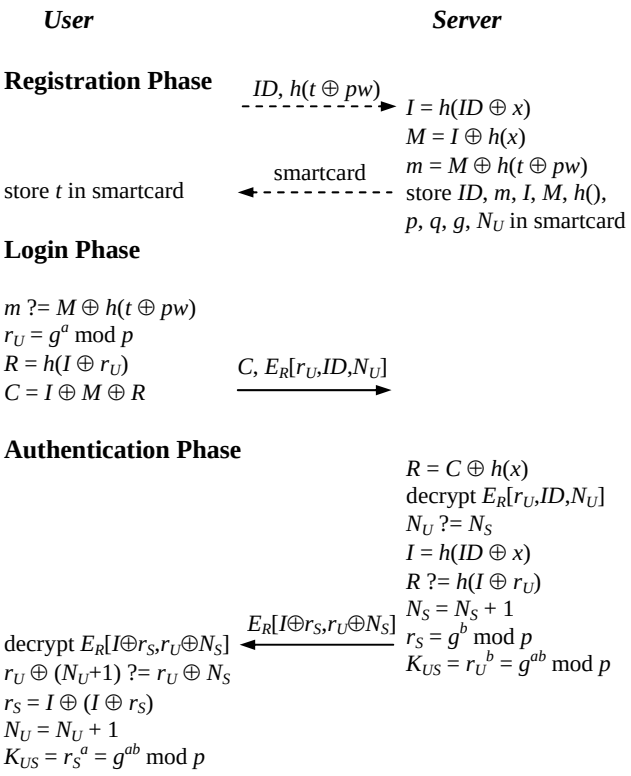

Fig. 1 Hu et al.'s scheme.

2.1 Registration phase

This phase works whenever a user U initially registers or re-registers to the remote server S.

(a) U chooses a password pw, generates a random number t, computes $h(t \oplus pw)$, and then submits his identity ID and $h(t \oplus pw)$ to S over secure channel.
(b) If it is U's initial registration, S creates an entry for U and stores ID and N_S in this entry. Otherwise, S updates the existing entry for U. Next S computes $I = h(ID \oplus x)$, $M = I \oplus h(x) = h(ID \oplus x) \oplus h(x)$ and $m = M \oplus h(t \oplus pw) = h(ID \oplus x) \oplus h(x) \oplus h(t \oplus pw)$, where x is the secret key of the remote server.
(c) S issues a smartcard containing ID, I, M, m, N_U, g, p, and $h()$ to U.
(d) U enters t into his/her smartcard. U does not have to remember t.

U and S respectively have a counter N_U and N_S so that the recipients can verify the timeliness of the messages and recognize and reject replays of messages communicated in the past. N_U and N_S are initially set and synchronized as 0.

2.2 Login phase

This phase works whenever U wants to login to S.

(a) U inserts his/her smartcard into a card reader and enters his/her identity ID and pw.
(b) After checking the validity of the ID and verifying whether $M \oplus h(t \oplus pw)$ and m equals, the smartcard generates a random number $r_U = g^a \bmod p$, and then computes $R = h(I \oplus r_U)$ and $C = I \oplus M \oplus R = h(x) \oplus R$.
(c) U sends the message C and $E_R[r_U, ID, N_U]$ to S, where the $E_R[r_U, ID, N_U]$ is encrypted with the secret key R.

2.3 Authentication phase

This phase works whenever S receives U's login request.

(a) S computes $R = C \oplus h(x)$ and then decrypts the message $E_R[r_U, ID, N_U]$ with the secret key R.

(b) After checking the validity of the *ID*, *S* compares N_U with the corresponding N_S. If they are equal, *S* continues the next step. Otherwise, *S* gives a synchronization signal to *U*, and then *U* must send an authentication request message to synchronize N_U with N_S.
(c) *S* computes $I = h(ID \oplus x)$ and verifies whether the following equation holds: $R ?= h(I \oplus r_U)$. If it holds, *S* accepts the service request and sets $N_S = N_S + 1$.
(d) *S* sends the message $E_R[I \oplus r_S, r_U \oplus N_S]$ to *U*, where $r_S = g^b \bmod p$.
(e) Upon receiving the message, *U* decrypts it with *R* and checks whether $r_U \oplus N_S ?= r_U \oplus (N_U + 1)$. If so, *U* computes $r_S = I \oplus (I \oplus r_S)$, sets $N_U = N_U + 1$, and then *U* can generate the session key $K_{US} = r_S^a = g^{ab} \bmod p$.

3. Weaknesses in Hu et al.'s scheme

Hu et al. pointed out that Chien and Chen's scheme has some problems as follows: it cannot resist strong server/user masquerading attack, insider attack, denial of service attack and restricted replay attack; it has a slow wrong password detection problem. So they proposed an improved scheme to solve these problems. Unfortunately, Hu et al.'s scheme is still vulnerable to strong server/user masquerading attack and denial of service attack and does not even provide user anonymity. Hu et al.'s scheme suffers from server/user masquerading attack in the case that the secret information stored in a legal user's smartcard or just the middle computation result can be obtained in some way. As described in Hu et al.'s scheme, we will call the attack a 'strong' one.

3.1 Strong user masquerading attack

In Hu et al.'s scheme, an attacker E is easily able to impersonate the user *U* who is legitimate. When *U* transmits a login request message to the remote server *S*, *E* intercepts the login request message and prevents the message and all *U*'s login request messages thereafter from being transmitted to *S* during impersonating *U*. Then, *E* tries to impersonate *U* by sending the intercepted login message to *S*. However, *S* will not recognize the attack and think *E*'s login as *U*'s without a doubt. *E* could not get the same session key as one generated by *S* through this attack. However, if an attacker *E* is one of legal users, he/she can obtain the same session key as one of *S* as follows:

(a) *E* obtains R_E and C_E from his/her own smartcard and then computes $h(x) = C_E \oplus R_E$.
(b) When a legal user *U* tries to login to *S*, *E* intercepts and blocks the login message C_U and $E_{R_U}[r_U, ID_U, N_U]$ of *U*, computes $R_U = C_U \oplus h(x)$ and gets ID_U and N_U by decrypting $E_{R_U}[r_U, ID_U, N_U]$ using R_U.
(c) *E* generates a random number *e*, computes $r_E = g^e \bmod p$, and then sends $E_{R_U}[r_E, ID_U, N_U]$ to *S*.
(d) After receiving the message, *S* checks the correctness of N_U and R_U but does not know the existence of *E*.
(e) Finally, *E* and *S* will compute the same session key $K_{ES} = g^{eb} \bmod p$.

3.2 Strong server masquerading attack

In Hu et al.'s scheme, if an attacker *E* is one of legal users who was issued a smartcard from the remote server *S*, he/she can impersonate *S* as follows. We assume that the owner of a smartcard could obtain the values stored and the middle results computed in the smartcard as described in Hu et al.'s scheme.

(a) *E* obtains C_E and R_E from his/her own smartcard and then computes $h(x) = C_E \oplus R_E$.
(b) After receiving the login message C_U and $E_{R_U}[r_U, ID_U, N_U]$ of a legal user *U*, *E* computes $R_U = C_U \oplus h(x)$ and decrypts $E_{R_U}[r_U, ID_U, N_U]$ using R_U.
(c) *E* generates a random number *e*, computes $E_{R_U}[e, r_U \oplus (N_U + 1)]$ and then sends it to *U*.
(d) *U* checks the correctness of $r_U \oplus (N_U + 1)$ after decrypting $E_{R_U}[e, r_U \oplus (N_U + 1)]$. However, *U* does not know the existence of *E*.

3.3 User anonymity

To provide the user anonymity, the protocol should not reveal the identity of users in the login and authentication phase. However, Hu et al.'s scheme does not provide the user anonymity, because *E* can easily obtain the identities of other legal users if *E* is one of legal users as described in the sub-section 3.2.

3.4 Denial of Service attack

An attacker *E* could succeed the denial of service attack when he/she causes legal users not to be able to login to *S* using their own smartcards from now on. Hu et al.'s scheme employed counters in the replace of timestamps using system clocks to prevent the restricted replay attack. In Hu et al.'s scheme, *U* and *S* respectively have the counters N_U and N_S, which are set and synchronized as 0 in the registration phase. And whenever *U* successfully logins to *S*, the counters are respectively increased by 1. However, if *E* succeeds the above user/server masquerading attack, the values of these counters will not be equal. Thereafter, it is impossible that *U* passes the authentication of *S* using his/her own smartcard. To solve

this problem, Hu et al.'s scheme merely mentioned that *S* gives a synchronization signal to *U* and then *U* has to send an authentication request message to synchronize N_U with N_S. However, the scheme did not describe it in detail. Therefore, it seems that Hu et al.'s scheme is difficult to avoid the denial of service attack.

3.5 A problem in actual operations

Most of smartcard-based remote authentication schemes including Chien and Chen's scheme have users who send their passwords in plaintext to the remote server in the registration phase. So, Hu et al. pointed out that they do not withstand sever insider attacks and made a trial to prevent this. In the registration phase of Hu el al.'s scheme, *U* sends $h(t \oplus pw)$ instead of plaintext password *pw*, where *t* is a random number and it is difficult to be memorized by a person. So, the scheme described that *U* has to store *t* into his/her own smartcard. However, this is not applicable in reality, because there is much time interval between when *U* generates *t* and when *U* stores *t* into the smartcard. Additionally, all users should own special devices to store *t* into smartcard without a support from the remote server.

4. Conclusion

This paper have shown that Hu et al.'s scheme is still vulnerable to strong server/user masquerading attack and denial of service attack and does not provide user anonymity. Furthermore, the scheme requires that the user should store a random number in his/her own smartcard after being issued the smartcard from the server in the user registration phase to prevent the insider attack. Additionally, we pointed out that this is not applicable in reality.

Acknowledgments

This research was supported by Ministry of Knowledge and Economy, Republic of Korea, under the ITRC(Information Technology Research Center) support program supervised by IITA(Institute for Information Technology Advancement) (IITA-2008-C1090-0801-0004).

References

[1] 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, pp. 629-631, 2004.

[2] H.Y. Chien and C.H. Chen, "A remote authentication scheme preserving user anonymity," *IEEE AINA*'05, Vol. 2, pp. 245-248, March 2005.

[3] L. Hu, Y.Yang, and X Niu. "Improved Remote User Authentication Scheme Preserving Anonymity," *Fifth Annual Conference on Communication Networks and Services Research(CNSR)*, pp. 323-328, 2007.

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

[5] H.M. Qiu, Y.X. Yang, and Z.M. Hu, "A new mutual user authentication scheme using smart card," *Application Research of Computers*, No. 12, pp. 103-105, 2005.

[6] E.J. Yoon and K.Y. Yoo, "More efficient and secure remote user authentication scheme using smart cards", *IEEE ICPADS'05*, Vol. 2, pp. 73-77, July 2005.

[7] C.C. Chang and T.C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, Vol. 138, No. 3, pp. 165-168, 1991.

[8] 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, pp. 28-30, 2000.

[9] W.S. Juang, "Efficient password authenticated key agreement using smart cards," *Computers and Security*, Vol. 23, No. 2, pp. 167-173, 2004.

[10] C.I. Fan, Y.C. Chan, and Z.K. Zhang, "Robust remote authentication scheme with smart cards," *Computers and Security*, Vol. 24, No.8, pp. 619-628, 2005.

Sung-Woon Lee received the BS and MS degrees in computer science from Chonnam National University, Korea in 1994 and 1996, respectively, and the Ph.D. degree in computer engineering from Kyungpook National University, Korea, in 2005. He was with the Korea Information System as a researcher, Korea, from 1996 to 2000. Currently, he is a professor in the department of information security, Tongmyong University, Korea. His research interests include cryptography, network security, and security protocol.

Hyuck-Jin Kwon received the BS degree in computer engineering from Kyungil University, Korea, in 2008. He is currently pursuing his MS course in information security from Tongmyong University, Korea. His research interests include security protocol and cryptography.

Hyun-Sung Kim received the BS degree in computer engineering from Kyungil University, Korea, in 1996 and the MS and Ph.D. degrees in computer engineering from Kyungpook National University, Korea, in 1998 and 2002, respectively. He was with the Ditto Technology as a senior researcher, Korea, from 2000 to 2002. Currently, he is a professor in the school of computer engineering, Kyungil University, Korea. His research interests include designing crypto-processor, network security, security protocol, and cryptography.