Cryptanalysis to a Remote User Authentication Scheme Using Smart Cards for Multi-server Environment^{*}

Youngsook Lee^{1,**}, Jeeyeon Kim², and Dongho Won^{2,***}

¹ Department of Cyber Investigation Police, Howon University, Korea
ysooklee@howon.ac.kr

² Department of Computer Engineering, Sungkyunkwan University, Korea
jeeyeonkim@paran.com, dhwon@security.re.kr

Abstract. Recently, Hsiang et al. proposed a remote user authentication scheme suited for multi-server environment, in which users can be authenticated anonymously using a smart card. This work reviews Hsiang et al.'s scheme and provides a security analysis on the scheme. Our analysis shows that Hsiang et al.'s scheme does not achieve its fundamental goal of not only any kind of authentication, either server-to-user authentication or user-to-server authentication but also password security. The contribution of the current work is to demonstrate these by mounting two attacks, a server impersonation attack and a user impersonation attack, on Hsiang et al.'s scheme. In addition, we demonstrate that their scheme is vulnerable to two-factor security which guarantees the security of the scheme when either the user's smart card or its password is stolen, but not both by employing the off-line dictionary attack.

Keywords: distributed system; authentication scheme; smart card; user anonymity; impersonation attack; off-line dictionary attack.

1 Introduction

In 2009, Hsiang et al. [2] proposed a remote user authentication scheme for multi-server environment in which users may send a login request message without disclosing their identities[5,7,11,3,9,8,10,13,1,6]. In addition to providing user anonymity, this scheme exhibits various other merits: (1) it allows the user to register only once with the registration center and then he/she is able to gain access to all servers included in multi-server environment without registering with every single server; (2) it does not require any server to maintain a password table for verifying the legitimacy of login users; (3) it allows users to choose and change their passwords according to their liking and hence gives more user

^{*} This work was supported by Howon University in 2011.

^{**} The first author.

^{***} Corresponding author.

convenience; (4) it does not require synchronized clocks between in the network by using random numbers called nonces; (5) it is extremely efficient in terms of the computational cost since the protocol participants perform only a few hash function operations.

However, in this article, we uncover that Hsiang et al.'s scheme does not guarantee its main security goal authenticating between a remote individual and the server. We show these by mounting two attacks, a server impersonation attack and a user impersonation attack on Hsiang et al.'s scheme. Besides reporting the two security flaws, we demonstrate that the scheme is vulnerable to two-factor security [12] which guarantees the security of the scheme when either the user's smart card or its password is stolen, but not both by employing the off-line dictionary attack. What we do in this work is to report these security vulnerabilities of Hsiang et al.'s scheme.

The remainder of this paper is organized as follows. We begin by reviewing goal authenticating et al.'s remote user authentication scheme in Section 2. Then in Section 3, we present security weaknesses in goal authenticating et al.'s authentication scheme. Finally, we conclude this work in Section 4.

2 Review of Hsiang et al.'s Authentication Scheme

This section reviews a remote user authentication scheme proposed by Hsiang et al. [2]. The scheme participants include a registration center, a remote user, and multiple service provider servers. For simplicity, we denote the registration center by RC , the remote user by U_i , and the servers by $S_1, S_2, \dots, S_n$. The scheme assumes that the registration center RC is a trust party responsible for securely delivering the secret keys to be shared with between U_i and S_j . Hsiang et al.'s scheme consists of two phases: registration phase and authentication phase. The registration phase is performed only once per user when a new user registers itself with the registration center. The authentication phase is carried out whenever a user wants to gain access to each server included in multi-server environment. Before the registration phase is performed for the first time, the registration center RC decides on the following system parameters: a one-way hash function h and three cryptographic keys x, y and r . The key y is shared securely among the registration center and all involved servers, while x and r are kept secret by the registration center.

2.1 Registration Phase

This is the phase where a new registration of a user takes place. The registration proceeds as illustrated by Fig. 1, where dashed lines indicate a secure channel:

Step 1. A user U_i , who wants to register with the registration center RC , chooses its password PW_i and a random number b at will. Then U_i computes $\pi_i = h(b||PW_i)$ and submits a registration request, consisting of its identity ID_i and π_i , to the registration center RC via a secure channel.

Fig. 1. The registration phase of Hsiang et al.'s scheme

Step 2. Upon receiving the request $\langle ID_i, \pi_i \rangle$, RC computes

$$\begin{aligned}
 K_i &= h(ID_i || x), \\
 M_i &= K_i \oplus h(ID_i || \pi_i), \\
 Z_i &= h(\pi_i || r) \oplus h(x \oplus r), \\
 V_i &= Z_i \oplus \pi_i, \\
 R_i &= h(\pi_i || r), \\
 H_i &= h(K_i).
 \end{aligned}$$

and issues a smart card containing $\langle M_i, V_i, H_i, R_i, h(\cdot) \rangle$ to U_i .

Step 3. Upon receiving the smart card, U_i enters the random number b into its smart card. Accordingly, b is additionally stored on the smart card.

2.2 Mutual Authentication Phase

This phase constitutes the core of the scheme and is performed whenever some user U_i wants to log on to the server S_j . U_i initiates this phase by inserting its smart card into a card reader and entering its password PW_i and identity ID_i and the server S_j 's identity ID_{S_j} . Given the user input, the smart card and the server perform the following steps as outlined in Fig. 2¹:

¹ N_{rj} was incorrectly stated as N_{jr} in the thirty fifth line of in page 1121 of [2]. We have corrected this typographical error.

Fig. 2. The mutual authentication phase of Hsiang et al.'s scheme

Step 1. Using the user-given PW_i and ID_i , the smart card computes $K_i = M_i \oplus h(ID_i || h(b \oplus PW_i))$ and $H'_i = h(K_i)$. Then the smart card checks that H'_i is equal to H_i . If they are equal, the smart card proceeds to the next step. Otherwise, the smart card aborts the authentication phase.

Step 2. The smart card chooses a random nonce u and computes

$$\begin{aligned} A_i &= V_i \oplus h(b \oplus PW_i), \\ CID_i &= h(b \oplus PW_i) \oplus h(K_i || A_i || u), \\ P_i &= K_i \oplus h(A_i || u || ID_{S_j}), \\ Q_i &= h(V_i || A_i || u), \\ C_i &= h(A_i || u + 1 || ID_{S_j}), \\ D_i &= R_i \oplus ID_{S_j} \oplus u. \end{aligned}$$

Then the smart card sends the login request message $\langle CID_i, P_i, Q_i, C_i, D_i, u \rangle$ to the server S_j .

Step 3. S_j first chooses a random number w and computes $L_j = H(ID_{S_j} || y) \oplus w$. Then, S_j sends the message $\langle L_j, ID_{S_j}, D_i, C_i, u \rangle$ to the registration center RC .

Step 4. When the message arrives, the registration center RC computes $w' = L_j \oplus h(ID_{S_j} || y)$, $R'_i = D_i \oplus ID_{S_j} \oplus u$, and $Z'_i = R'_i \oplus h(x \oplus r)$. Then RC verifies that C_i equals $h(Z'_i || u + 1 || ID_{S_j})$. If this condition is untrue, RC rejects the login request. Otherwise, RC generates a new random nonce n , computes $E_i = h(w' || h(ID_{S_j} || y) || n)$, $F_i = Z'_i \oplus h(h(ID_{S_j} || y) \oplus w')$ and sends the response message $\langle E_i, F_i, n \rangle$ to the server S_j .

Step 5. After receiving $\langle E_i, F_i, n \rangle$, S_j chooses a random number t and computes

$$\begin{aligned} A'_i &= F_i \oplus h(h(ID_{S_j} || y) \oplus w), \\ K'_i &= P_i \oplus h(A'_i || u || ID_{S_j}), \\ \pi'_i &= CID_i \oplus h(K'_i || A'_i || u), \\ V'_i &= A'_i \oplus \pi'_i, \\ G_i &= h(V'_i || u || A'_i || ID_{S_j}). \end{aligned}$$

Then, the server S_j checks that : (1) E_i is equal to $h(w || h(ID_{S_j} || y) || n)$ and (2) Q_i is equal to $h(V'_i || A'_i || u)$. If both of theses conditions hold, S_j believes U_i as authentic. Otherwise, S_j aborts its authentication attempt. After that, S_j sends the response message $\langle G_i, t \rangle$ to U_i .

Step 6. Having received G_i from S_j , U_i verifies the correctness of G_i by checking that G_i equals $h(V_i || u || A_i || ID_{S_j})$. If correct, U_i accepts the response message, computes $J_i = h(V_i || t || A_i || ID_{S_j})$, and sends the message $\langle J_i \rangle$ to S_j ; otherwise, reject it.

Step 7. After receiving $\langle J_i \rangle$, S_j verifies the correctness of J_i by checking that J_i equals $h(V'_i || t || A'_i || ID_{S_j})$. If correct, S_j believes as the legitimate user; otherwise, reject it.

Finally, U_i and S_j compute their session key SK as

$$SK = h(V_i || A_i || u || t || ID_{S_j}).$$

3 Cryptanalysis of Hsiang et al.'s Scheme

In this section we point out that Hsiang et al.'s scheme not only does not achieve its main security goal of authenticating between a remote individual and the server but also password security. In addition, we found that the scheme does not provide two-factor security.

3.1 Attacks against Mutual Authentication

Unfortunately, Hsiang et al.'s remote user authentication scheme supports neither user-to-server authentication nor server-to-user authentication. In this subsection, we show this by presenting two impersonation attacks, a user impersonation attack and a server impersonation attack. The user impersonation attack and the server impersonation attack are given to violate respectively user-to-server and server-to-user authentications of Hsiang et al.'s scheme.

Impersonating U_i to S_j . First, we present a user impersonation attack where an attacker U_a , who is a legitimate user registered with the registration center, can easily impersonate the remote user U_i to any other server S_j . Before describing the attack, we note that the secret values stored in a smart card could be extracted by monitoring its power consumption [4,8]. We now proceed to describe the user impersonation attack.

1. As a preliminary step, the attacker U_a extracts the secret values b , V_a and R_a stored in its smart card. From V_a and its hashed password value π_a , U_a recovers the value of $h(x \oplus r)$ as $h(x \oplus r) = V_a \oplus \pi_a \oplus R_a$.
2. Now when U_i initiates the authentication phase with the login request message $\langle CID_i, P_i, Q_i, C_i, D_i, u \rangle$, the attacker U_a posing as U_i intercepts this login request and sends to S_j a forged login message as follows: U_a who has obtained the login message, CID_i , P_i , u , D_i , and the secret value $h(x \oplus r)$, first, U_a chooses three random numbers, α , β , and PW'_i , and computes

$$\begin{aligned}
 R_i &= D_i \oplus ID_{S_j} \oplus u, \\
 A_i &= R_i \oplus h(x \oplus r), \\
 K_i &= P_i \oplus h(A_i || u || ID_{S_j}), \\
 CID_i^* &= h(\beta \oplus PW'_i) \oplus h(K_i || A_i || \alpha), \\
 P_i^* &= K_i \oplus h(A_i || \alpha || ID_{S_j}), \\
 V_i^* &= A_i \oplus h(\beta \oplus PW'_i), \\
 Q_i^* &= h(V_i^* || A_i || \alpha), \\
 C_i^* &= h(Z_i || \alpha + 1 || ID_{S_j}), \\
 D_i^* &= R_i \oplus ID_{S_j} \oplus \alpha.
 \end{aligned}$$

Then U_a posing as some registered user U_i sends the forged login request message $\langle CID_i^*, P_i^*, Q_i^*, C_i^*, D_i^*, \alpha \rangle$ as a login request message to the server S_j .

3. After receiving $\langle CID_i^*, P_i^*, Q_i^*, C_i^*, D_i^*, \alpha \rangle$, the server S_j chooses a random number w and computes $L_j = H(ID_{S_j} || y) \oplus w$. Then, S_j sends the message $\langle L_j, ID_{S_j}, D_i^*, C_i^*, \alpha \rangle$ to the registration center RC .
4. Since, from RC 's point view, D_i^*, C_i^*, α are indistinguishable from D_i, C_i, u of an honest execution, RC believes that the message $\langle D_i^*, C_i^*, \alpha \rangle$ is from U_i . Hence, RC operates as specified in protocol using the received messages from S_j . First, RC computes w' , R'_i , Z'_i and proceeds to verify the authenticity of the login request. That is, RC computes $w' = L_j \oplus h(ID_{S_j} || y)$, $R'_i = D_i^* \oplus ID_{S_j} \oplus u$, and $Z'_i = R'_i \oplus h(x \oplus r)$ and checks that C_i^* equals $h((Z'_i || \alpha + 1 || ID_{S_j}))$. Since it holds, RC will welcome U_a 's visit to the system. Then, RC chooses a random number n , computes $E_i = h(w' || h(ID_{S_j} || y) || n)$ and $F_i = Z'_i \oplus h(h(ID_{S_j} || y) \oplus w)$ and sends the response message $\langle E_i F_i, n \rangle$ to S_j .
5. Since E_i , A'_i , and Q_i are all valid, everything proceeds as usual. In response to U_a 's login message, S_j chooses a random number t , computes $G_i = h(V'_i || u || A'_i || ID_{S_j})$, and sends $\langle G_i, t \rangle$ to U_a .
6. Now, an attacker U_a upon receiving G_i and t from S_j , computes $J_i = h(V_i || t || A_i || ID_{S_j})$, and sends the response message $\langle J_i \rangle$ to S_j . Because J_i equals $h(V' || t || A'_i || ID_{S_j})$, S_j will be unaware of attack and believes U_a as legitimate user U_i .

Impersonating S_j to U_i . Now, we present a server impersonation attack where an attacker U_a , who is a legitimate user registered with the registration center, can easily impersonate the remote server S_j to any other registered user U_i . Before describing the attack, we note that the secret values stored in a smart card could be extracted by monitoring its power consumption [4,8]. We now proceed to describe the server impersonation attack.

1. As a preliminary step, the attacker U_a extracts the secret values b , V_a and R_a stored in its smart card. From V_a and its hashed password value π_a , U_a recovers the value of $h(x \oplus r)$ as $h(x \oplus r) = V_a \oplus \pi_a \oplus R_a$.
2. When U_i initiates the authentication phase with the login request message $\langle CID_i, P_i, Q_i, C_i, D_i, u \rangle$, the attacker U_a posing as S_j intercepts this message and sends a forged the server S_j 's response message as follows: U_a who has obtained the login message, CID_i, P_i, Q_i, D_i, u and the secret value, $h(x \oplus r)$, first
 - (a) generates a random number γ .
 - (b) computes

$$\begin{aligned}
 R_i &= D_i \oplus ID_{S_j} \oplus u, \\
 A'_i &= R_i \oplus h(x \oplus r), \\
 K'_i &= P_i \oplus h(A'_i || u || ID_{S_j}), \\
 V'_i &= A'_i \oplus CID_i \oplus h(K'_i || A'_i || u), \\
 G_a &= h(V'_i || u || A'_i || ID_{S_j}).
 \end{aligned}$$

- (c) and then sends $\langle G_a, \gamma \rangle$ in response to U_i 's login request.
3. The forged response $\langle G_a, \gamma \rangle$ will pass the verification test by U_i since G_i is equal to $h(V_i || u || A_i || ID_{S_j})$. Hence, U_i believes U_a as the authentic server.

Security Analysis. It is clear that the vulnerability of Hsiang et al.'s scheme to two attacks above is mainly because the same hash value $h(x \oplus r)$ is used in computing Z_i for all users U_i : $Z_i = h(\pi_i || r) \oplus h(x \oplus r)$ for all i . This oversight allows the attacker to derive $h(x \oplus r)$ easily from Z_i by using the extracted value $R_i (= h(PW_i || r))$ from its smart card and then creates the vulnerability to two impersonation attacks. Based on this observation, anyone who knows the value of $h(x \oplus r)$ stored in its smart card is able to compute a valid login request $CID_i = h(b \oplus PW_i) \oplus h(K_i || A_i || u)$ (even without knowing U_i 's password PW_i) or able to compute a valid response $G_i = h(V_i' || u || A_i' || ID_{S_j})$ (even without knowing the server's secret values x and r).

3.2 Attack against Two-Factor Security

Loosely stated, two-factor security [12] means that the security of the scheme is provided when either the user's smart card or its password is stolen, but not both. Hsiang et al. [2] claim that their authentication scheme achieves two-factor security.

Assume that the attacker, who is a legitimate user registered with the registration center, has stolen the U_i 's smart card or gained access to it and extracted the secret values stored in it by monitoring its power consumption [4,8]. Now the attacker U_a has obtained the value π_i stored in the U_i 's smart card. Then the following description represents our off-line dictionary attack mounted by the attacker U_a against U_i 's password: The attacker U_a , who wants to find out PW_i , now guesses possible passwords and checks them for correctness.

1. As a registered user, the attacker U_a , who has obtained R_a stored in its smart card, learns the value of $h(x \oplus r)$ by computing $h(x \oplus r) = V_a \oplus \pi_a \oplus R_a$ using its password PW_a .
2. Using V_i and R_i from U_i and $h(x \oplus r)$ from itself, U_a computes $h(b \oplus PW_i) = V_i \oplus R_i \oplus h(x \oplus r)$.
3. Next, U_a makes a guess PW_i' for PW_i and computes $h(b \oplus PW_i')$.
4. U_a then verifies the correctness of PW_i' by checking the equality $h(b \oplus PW_i') = h(b \oplus PW_i)$. Notice that if PW_i' and PW_i are equal, then $h(b \oplus PW_i') = h(b \oplus PW_i)$ ought to be satisfied.
5. U_a repeats steps (3) and (4) until a correct password is found.

The two above security vulnerabilities of Hsiang et al.'s scheme are attributed to the following a flaw in its design:

- The same hash value $h(x \oplus r)$ is used in computing Z_i for all users U_i : $Z_i = h(\pi_i || r) \oplus h(x \oplus r)$ for all i .

4 Conclusion

We have analyzed the security of the smart card based user authentication scheme proposed by Hsiang et al. [2]. Our security analysis uncovered that Hsiang

et al.'s scheme does not achieve its main security goal not only of authenticating between a remote individual and the server but also of password security. Now, the failure of Hsiang et al.'s scheme to achieve authentication has been made clear through two attacks, a server impersonation attack and a user impersonation attack, on the scheme. The server impersonation attack and the user impersonation attack have been considered to infringe respectively server-to-user and user-to-server authentications of the scheme. In addition, we demonstrate that Hsiang et al.'s scheme fails to provide two-factor security which guarantees the security of the scheme when either the user's smart card or its password is stolen, but not both by employing the off-line dictionary attack.

References

1. Chang, C., Lee, J.S.: An efficient and secure multi-server password authentication scheme using smart cards. In: *Proceeding of the International Conference on Cyberworlds*, IEEE, Los Alamitos (2004)
2. Hsiang, H.-C., Shih, W.-K.: Improvement of the secure dynamic Id based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces* 31, 1118–1123 (2009)
3. Juang, W.S.: Efficient multi-server password authenticated key agreement using smart cards. *IEEE Trans. Consum. Electron.* 50(1), 251–255 (2004)
4. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) *CRYPTO 1999*. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
5. Li, L.-H., Lin, I.-C., Hwang, M.-S.: A remote password authentication scheme for multi-server architecture using neural networks. *IEEE Trans. on Neural Networks* 12(6), 1498–1504 (2001)
6. Liao, Y.-P., Wang, S.-S.: A secure dynamic ID based remote user authentication scheme for multi-server environment, *Computer Standards & Interfaces* (2007) (article in press)
7. Lin, I.-C., Hwang, M.-S., Li, L.-H.: A new remote user authentication scheme for multi-server internet environments. *Future Generation Computer System* 19, 13–22 (2003)
8. Messergers, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart card security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5), 541–552 (2002)
9. Tsuar, W.-J.: An enhanced user authentication scheme for multi-server internet services. *Appl. Math. Comput.* 170, 258–266 (2005)
10. Tsuar, W.-J., Wu, C.-C., Lee, W.-B.: A flexible user authentication scheme for multi-server internet services. In: Lorenz, P. (ed.) *ICN 2001*. LNCS, vol. 2093, pp. 174–183. Springer, Heidelberg (2001)
11. Tsaur, W.-J., Wu, C.-C., Lee, W.-B.: A smart card-based remote scheme for password authentication in multi-server Internet services. *Computer Standards & break Interfaces* 27, 39–51 (2004)
12. Tian, X., Zhu, R.W., Wong, D.S.: Improved efficient remote user authentication schemes. *Int. J. Netw. Secur.* 4(2), 149–154 (2007)
13. Yang, Y., Wang, S., Bao, F., Wang, J., Deng, R.: New efficient user identification and key distribution scheme providing enhanced security. *Comput. Secur.* 23(8), 697–704 (2004)