TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 10, October 2014, pp. 7412 ~ 7421
DOI: 10.11591/telkomnika.v12i8.5407

Cryptanalysis and Improvement of an Authentication Scheme for Telecare Medical Information Systems

Yun Zhao[1]*, Wenbo Shi[2]
[1]School of Information Engineering, Guangdong Medical College, Guangdong, China
[2]Department of Electronic Engineering, Northeastern University at Qinhuangdao, Qinhuangdao, China
*Corresponding author, e-mail: zhaoyun2012@hotmail.com

Abstract

The telecare medical information system (TMIS) could improve quality of medical care since it allows patients to enjoy health-care delivery services in their home. However, the privacy and security influence the development of the TMIS since it is employed in open networks. Recently, Wu and Xu proposed a privacy authentication scheme for the TMIS and claimed that their scheme could overcome weaknesses in previous schemes. However, we will demonstrate that their scheme is venerable to the server spoofing attack and cannot provide user anonymity. To overcome weaknesses in their scheme, we also propose a new authentication scheme for the TMIS. Analysis shows that our scheme not only overcome weaknesses in Wu et al.'s scheme, but also has better performance.

Keywords*: mutual authentication, anonymity, smart card, telecare medical information system*

1. Introduction

With the rapid development of technologies in wireless communication, low-power integrated circuits and wearable medical sensors, the telecare medical information system (TMIS) is widely used to improve quality of medical care. Through TMIS, patients could login the remote server and enjoy various medical services almost anywhere at any time. Therefore, the TMIS could bring great convenience to people's life. How to address the privacy and security in the TMIS has attracted wide attention since the data transmitted in the TMIS is very sensitive and important.

The anonymity authentication scheme could provide mutual authentication between the user and the remote server and user anonymity. Then, it is very suitable for solve security problem in the TMIS. In 1981, Lamport [1] proposed the first authentication scheme for secure communication in open networks. However, Lamport's scheme is vulnerable to the stolen verifier table attack. Since then, many authentication schemes [2-10] have been proposed for different applications. However, those schemes [1-10] are not for the TMIS since their performance is not satisfactory. To solve the problem, Wu et al. [11] proposed the first authentication scheme for TMIS. Unfortunately, He et al. [12] pointed out that Wu et al.'s scheme is vulnerable to the impersonation attacks and the insider attack. He et al. [12] also proposed a new authentication scheme for TMIS. Later, Wei et al. [13] pointed out that Wu et al.'s scheme and He et al.'s scheme cannot provide two-factor security. Wei et al. also proposed an improved scheme and claimed that their scheme could withstand various attacks. However, Zhu [14] demonstrated that Wei et al.'s scheme is vulnerable to the off-line password guessing attack.

All those authentication schemes for TMIS cannot provide user anonymity since users' identities are transmitted in plaintext format. Das et al. [15] proposed a dynamic ID-based authentication scheme to protect user's anonymity. In 2012, Chen et al. [16] proposed a dynamic ID-based authentication scheme for TMIS. However, Cao et al. [17], Xie et al. [18], Lin [19] and Jiang et al. [20] pointed out that Chen et al.'s scheme had weaknesses such as off-line password guessing attack, tracking attack, lack of privacy protection and so on. Jiang et al. [20] also proposed an improved scheme to overcome weaknesses in previous schemes. However, Wu and Xu [21] pointed out that Jiang et al.'s scheme has useless identity and is vulnerable to off-line password guessing attack, user impersonation attack and Denial of Service (DoS)

Received December 19, 2013; Revised July 2, 2014; Accepted July 25, 2014

attack. Wu and Xu also proposed an improved scheme to protect the user's privacy in TMIS. Unfortunately, we will demonstrate that Wu and Xu's scheme is venerable to the server spoofing attack and cannot provide user anonymity. We also proposed a new authentication scheme for TMIS to overcome weaknesses in their scheme. Analysis shows that our scheme not only overcome in Wu et al.'s scheme, but also has better performance.

The organization of the paper is described as follows. In Section "Review of Wu and Xu's scheme", we briefly review their scheme. Then the Section "Security analysis of Wu and Xu's scheme" analyzes security of Wu and Xu's scheme. In Section "Our proposed scheme", we propos a new authentication scheme for TMIS. Sections "Security analysis" and "Performance analysis" analyze the security and performance of our scheme separately. Some conclusions are proposed in the last section.

2. Review of Wu and Xu's scheme

In this section, we will give a brief review of Wu and Xu et al.'s scheme. For convenience, some notations are defined as follows.

a) U_i : a user;

b) ID_i : the identity of U_i ;

c) PW_i : the password of U_i ;

d) S : the remote server for the system;

e) x : the secret key of S ;

f) T_i : the timestamp generated by U_i ;

g) T_S : the timestamp generated by S ;

h) N : the registration times of U_i ;

i) sk : the session key generated between U_i and S ;

j) $E_k(M)$: Encryption of a message M using the key k ;

k) $D_k(C)$: Decryption of a message C using the key k ;

l) $h(\cdot)$: a secure one-way hash function;

m) $\oplus$: the bitwise XOR operation;

n) ||: the concatenation operation;

Wu and Xu's scheme consists of five phases, i.e. the registration phase, the login phase, the authentication phase, the password change phase and the lost smart card revocation phase. The details are described as follows:

2.1. Registration Phase

In this phase, U_i could register or re-register at the remote S through the following step.

1) U_i generates a random number r_i, chooses his identity ID_i, password PW_i, computes $HPW_i = h(r_i \| PW_i)$ and sends the message $\{ID_i, HPW_i\}$ to S through a secure channel.

2) After receiving $\{ID_i, HPW_i\}$, S checks the validity of ID_i. If it is not valid, S rejects the session; otherwise, S checks the account records in database. If U_i is a new user, S adds the tuple $(ID_i, N = 0)$ into the database; otherwise, S sets $N = N + 1$ and stores it. Then S computes $J_i = h(x \| ID_i \| N)$, $L_i = J_i \oplus RPW_i$ and $E_i = h(x) \oplus h(RPW_i \| ID_i)$. At last, S stores $\{L_i, E_i, h(\cdot), E_k(\cdot), D_k(\cdot)\}$ into a smart card and sends it to U_i through a secure channel.

3) After receiving the smart card, U_i inputs r_i into it.

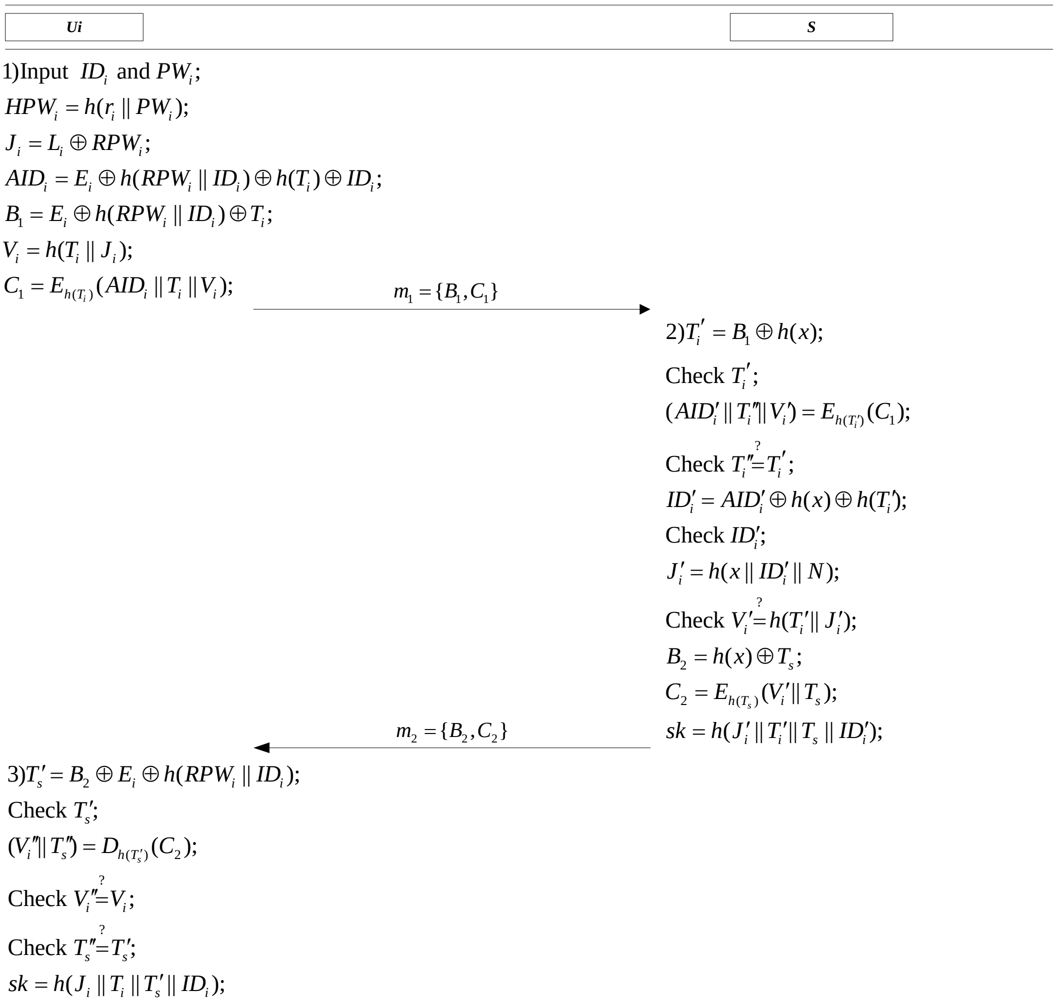
2.2. Login Phase

When wanting to login at S and enjoy services, as shown in Figure 1, U_i will carry out the following steps.

1) U_i inserts his smart card into a card reader and inputs his identity ID_i and password PW_i.

2) The smart card computes $HPW_i = h(r_i \| PW_i)$, $J_i = L_i \oplus RPW_i$, $AID_i = E_i \oplus h(RPW_i \| ID_i) \oplus h(T_i) \oplus ID_i$, $B_1 = E_i \oplus h(RPW_i \| ID_i) \oplus T_i$, $V_i = h(T_i \| J_i)$ and $C_1 = E_{h(T_i)}(AID_i \| T_i \| V_i)$, where T_i is the timestamp generated by U_i. At last, U_i sends the message $m_1 = \{B_1, C_1\}$ to S.

2.3. Authentication Phase



1)Input ID_i and PW_i;
$HPW_i = h(r_i \| PW_i)$;
$J_i = L_i \oplus RPW_i$;
$AID_i = E_i \oplus h(RPW_i \| ID_i) \oplus h(T_i) \oplus ID_i$;
$B_1 = E_i \oplus h(RPW_i \| ID_i) \oplus T_i$;
$V_i = h(T_i \| J_i)$;
$C_1 = E_{h(T_i)}(AID_i \| T_i \| V_i)$;

$m_1 = \{B_1, C_1\}$

2)$T_i' = B_1 \oplus h(x)$;
Check T_i';
$(AID_i' \| T_i'' \| V_i') = E_{h(T_i')}(C_1)$;
Check $T_i'' \overset{?}{=} T_i'$;
$ID_i' = AID_i' \oplus h(x) \oplus h(T_i')$;
Check ID_i';
$J_i' = h(x \| ID_i' \| N)$;
Check $V_i' \overset{?}{=} h(T_i' \| J_i')$;
$B_2 = h(x) \oplus T_s$;
$C_2 = E_{h(T_s)}(V_i' \| T_s)$;
$sk = h(J_i' \| T_i' \| T_s \| ID_i')$;

$m_2 = \{B_2, C_2\}$

3)$T_s' = B_2 \oplus E_i \oplus h(RPW_i \| ID_i)$;
Check T_s';
$(V_i'' \| T_s'') = D_{h(T_s')}(C_2)$;
Check $V_i'' \overset{?}{=} V_i$;
Check $T_s'' \overset{?}{=} T_s'$;
$sk = h(J_i \| T_i \| T_s' \| ID_i)$;

Figure 1. Wu and Xu's Scheme

As shown in Figure 1, U_i and S could authenticate each other through executing the following steps.

1) After receiving $m_1 = \{B_1, C_1\}$, S computes $T_i' = B_1 \oplus h(x)$ and checks whether T_i' is fresh. If it is not fresh, S stops the request; otherwise, S computes $(AID_i' \| T_i'' \| V_i') = E_{h(T_i')}(C_1)$. S checks whether T_i'' and T_i' are equal. If they are not equal, S stops the request; otherwise, S computes $ID_i' = AID_i' \oplus h(x) \oplus h(T_i')$ and checks whether ID_i' is in the account table. If it is not in the account table, S stops the session; otherwise, S computes $J_i' = h(x \| ID_i' \| N)$ and

checks whether V_i' and $h(T_i'\|J_i')$ are equal. If they are not equal, S stops the request; otherwise, S computes $B_2=h(x)\oplus T_s$, $C_2=E_{h(T_s)}(V_i'\|T_s)$, $sk=h(J_i'\|T_i'\|T_s\|ID_i')$ and sends the message $m_2=\{B_2,C_2\}$ to U_i , where T_s is the timestamp generated by S .

2) After receiving $m_2=\{B_2,C_2\}$, U_i computes $T_s'=B_2\oplus E_i\oplus h(RPW_i\|ID_i)$ and checks the freshness of T_s' . If it is not fresh, U_i stops the session; otherwise, U_i computes $(V_i''\|T_s'')=D_{h(T_s')}(C_2)$. Then U_i checks whether the equations $V_i''=V_i$ and $T_s''=T_s'$ hold. If either of them does not hold, U_i stops the session; otherwise, U_i computes $sk=h(J_i\|T_i\|T_s'\|ID_i)$.

2.4. Password Change Phase

When U_i wants to change his password, he inserts his smart card into a card reader and inputs his identity ID_i , the old password PW_i and a new password PW_i^{new} . Then step 2) of the login phase and step 1) of the authentication phase are executed.

After receiving $m_2=\{B_2,C_2\}$, U_i computes $T_s'=B_2\oplus E_i\oplus h(RPW_i\|ID_i)$ and checks the freshness of T_s' . If it is not fresh, U_i stops the session; otherwise, U_i computes $(V_i''\|T_s'')=D_{h(T_s')}(C_2)$. Then U_i checks whether the equations $V_i''=V_i$ and $T_s''=T_s'$ hold. If either of them does not hold, U_i stops the session; otherwise, U_i computes $HPW_i^{new}=h(r_i\|PW_i^{new})$, $L_i^{new}=L_i\oplus RPW_i\oplus RPW_i^{new}$ and $E_i^{new}=E_i\oplus h(RPW_i\|ID_i)\oplus h(RPW_i^{new}\|ID_i)$. At last, U_i replaces L_i and E_i with L_i^{new} and E_i^{new} separately.

2.5. Lost Smart Card Revocation Phase

When U_i loses his smart card, he can re-register at S through the secure channel as the registration phase. S verifies U_i , makes $N=N+1$ and stores (ID_i,N) into the account table. At last, S issues a new smart card to U_i .

3. Security Analysis of Wu and Xu's Scheme

Wu and Xu claimed that their scheme could withstand various attacks. However, in this section, we will show their scheme cannot provide user's anonymity and is vulnerable to the server spoofing attack.

Suppose U_a is a malicious user. Then he could get a smart card containing the message $\{L_i,E_i,h(\cdot),E_k(\cdot),D_k(\cdot)\}$ through registering at S , where, $L_a=h(x\|ID_a\|N)\oplus RPW_a$, $E_a=h(x)\oplus h(RPW_a\|ID_a)$ and $HPW_a=h(r_a\|PW_a)$. Since the messages are transmitted in public channel, we could assume that U_a has total control over the channel, i.e. he could intercept, insert and modify messages transmitted between the user and the server.

3.1. User Anonymity

User anonymity is very important it the TMIS since the leakage of user's identity could influence user's privacy. Wu and Xu claimed that their scheme could provide user's anonymity. However, in this section, we will show a malicious U_a could get other user's identity. The detail is described as follows.

1) U_a extracts $\{L_i,E_i\}$ from his smart card, where $HPW_a=h(r_a\|PW_a)$, $L_a=h(x\|ID_a\|N)\oplus RPW_a$ and $E_a=h(x)\oplus h(RPW_a\|ID_a)$.

2) U_a computes $HPW_a=h(r_a\|PW_a)$ and $h(x)=E_a\oplus h(RPW_a\|ID_a)$.

3) U_a intercepts $m_1=\{B_1,C_1\}$ sent U_i , where $AID_i=h(x)\oplus h(T_i)\oplus ID_i$, $C_1=E_{h(T_i)}(AID_i\|T_i\|V_i)$, $B_1=h(x)\oplus T_i$ and $V_i=h(T_i\|J_i)$.

4) U_a computes $T_i = B_1 \oplus h(x)$, $(AID_i \| T_i \| V_i) = D_{h(T_i)}(C_1)$ and $ID_i = AID_i \oplus h(x) \oplus h(T_i)$.

From the above description, we know that U_a could get the identity of U_i easily. Therefore, Wu and Xu's scheme cannot provide user anonymity.

3.2. Server Spoofing Attack

Wu and Xu claimed that their scheme could withstand various attacks. In this subsection, we will show their scheme is vulnerable to the server spoofing attack, i.e. a malicious user U_a could impersonate the sever to another user U_i. The details are described as follows.

1) U_a extracts $\{L_i, E_i\}$ from his smart card, where $HPW_a = h(r_a \| PW_a)$, $L_a = h(x \| ID_a \| N) \oplus RPW_a$ and $E_a = h(x) \oplus h(RPW_a \| ID_a)$.

2) U_a computes $HPW_a = h(r_a \| PW_a)$ and $h(x) = E_a \oplus h(RPW_a \| ID_a)$.

3) U_a intercepts $m_1 = \{B_1, C_1\}$ sent U_i, where $AID_i = h(x) \oplus h(T_i) \oplus ID_i$, $C_1 = E_{h(T_i)}(AID_i \| T_i \| V_i)$, $B_1 = h(x) \oplus T_i$ and $V_i = h(T_i \| J_i)$.

4) U_a computes $T_i' = B_1 \oplus h(x)$, $(AID_i' \| T_i'' \| V_i') = E_{h(T_i')}(C_1)$, $B_2 = h(x) \oplus T_s$, $C_2 = E_{h(T_s)}(V_i' \| T_s)$, and sends the message $m_2 = \{B_2, C_2\}$ to U_i.

It is easy to verify that the message $m_2 = \{B_2, C_2\}$ could pass U_i's verification. Therefore, U_a could impersonate S to U_i successfully and Wu and Xu's scheme is vulnerable to the server spoofing attack.

4. Our Proposed Scheme

To overcome weaknesses in Wu and Xu's scheme, we proposed an improved authentication scheme for TMIS. Our scheme also consists of five phases, i.e. the registration phase, the login phase, the authentication phase, the password change phase and the lost smart card revocation phase. The details are described as follows:

4.1. Registration Phase

In this phase, U_i could register or re-register at the remote S through the following step.

1) U_i generates a random number r_i, chooses his identity ID_i, password PW_i, computes $HPW_i = h(r_i \| PW_i)$ and sends the message $\{ID_i, HPW_i\}$ to S through a secure channel.

2) After receiving $\{ID_i, HPW_i\}$, S checks the validity of ID_i. If it is not valid, S rejects the session; otherwise, S checks the account records in database. If U_i is a new user, S adds the tuple $(ID_i, N = 0)$ into the database; otherwise, S sets $N = N + 1$ and stores it. Then S generates a pseudo identity pid_i, computes $I_i = h(x \| pid_i)$, $J_i = h(x \| ID_i \| N)$, $E_i = I_i \oplus h(RPW_i \| ID_i)$ and $L_i = J_i \oplus RPW_i$. At last, S stores $\{pid_i, L_i, E_i, h(\cdot), E_k(\cdot), D_k(\cdot)\}$ into a smart card and sends it to U_i through a secure channel.

3) After receiving the smart card, U_i inputs r_i into it.

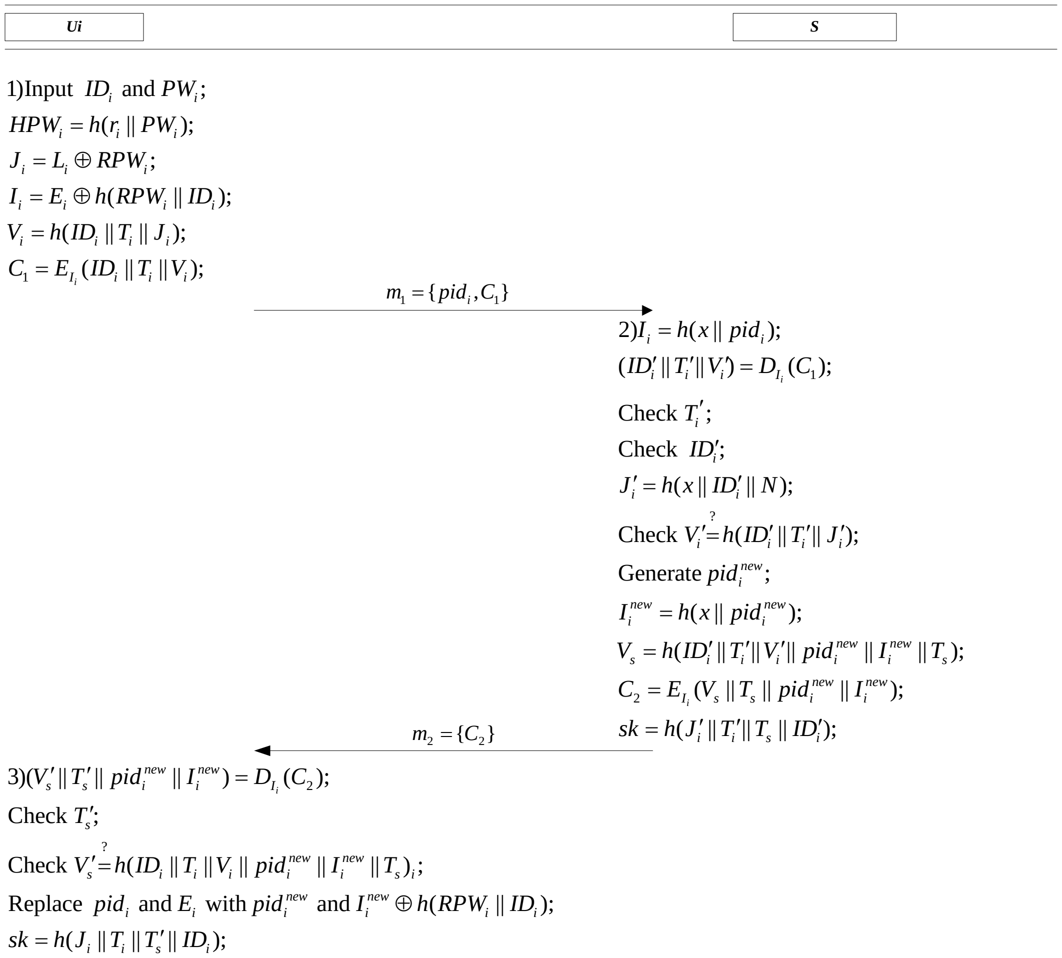
4.2. Login Phase

When wanting to login at S and enjoy services, as shown in Fig. 1, U_i will carry out the following steps.

1) U_i inserts his smart card into a card reader and inputs his identity ID_i and password PW_i.

2) The smart card computes $HPW_i = h(r_i \| PW_i)$, $J_i = L_i \oplus RPW_i$, $I_i = E_i \oplus h(RPW_i \| ID_i)$, $V_i = h(ID_i \| T_i \| J_i)$ and $C_1 = E_{I_i}(ID_i \| T_i \| V_i)$, where T_i is the timestamp generated by U_i. Then, U_i sends the message $m_1 = \{pid_i, C_1\}$ to S.

4.3. Authentication Phase



Ui

S

1)Input ID_i and PW_i;

$HPW_i = h(r_i \| PW_i)$;

$J_i = L_i \oplus RPW_i$;

$I_i = E_i \oplus h(RPW_i \| ID_i)$;

$V_i = h(ID_i \| T_i \| J_i)$;

$C_1 = E_{I_i}(ID_i \| T_i \| V_i)$;

$\xrightarrow{m_1 = \{pid_i, C_1\}}$

2)$I_i = h(x \| pid_i)$;

$(ID_i' \| T_i' \| V_i') = D_{I_i}(C_1)$;

Check T_i';

Check ID_i';

$J_i' = h(x \| ID_i' \| N)$;

Check $V_i' \overset{?}{=} h(ID_i' \| T_i' \| J_i')$;

Generate pid_i^{new};

$I_i^{new} = h(x \| pid_i^{new})$;

$V_s = h(ID_i' \| T_i' \| V_i' \| pid_i^{new} \| I_i^{new} \| T_s)$;

$C_2 = E_{I_i}(V_s \| T_s \| pid_i^{new} \| I_i^{new})$;

$sk = h(J_i' \| T_i' \| T_s \| ID_i')$;

$\xleftarrow{m_2 = \{C_2\}}$

3)$(V_s' \| T_s' \| pid_i^{new} \| I_i^{new}) = D_{I_i}(C_2)$;

Check T_s';

Check $V_s' \overset{?}{=} h(ID_i \| T_i \| V_i \| pid_i^{new} \| I_i^{new} \| T_s)_i$;

Replace pid_i and E_i with pid_i^{new} and $I_i^{new} \oplus h(RPW_i \| ID_i)$;

$sk = h(J_i \| T_i \| T_s' \| ID_i)$;

Figure 2. Our Scheme

As shown in Figure 2, U_i and S could authenticate each other through executing the following steps.

1) After receiving $m_1 = \{pid_i, B_1, C_1\}$, S computes $I_i = h(x \| pid_i)$, $(ID_i' \| T_i' \| V_i') = D_{I_i}(C_1)$ and checks whether T_i' is fresh. If it is not fresh, S stops the request; otherwise, S checks whether ID_i' is in the account table. If it is not in the account table, S stops the session; otherwise, S computes $J_i' = h(x \| ID_i' \| N)$ and checks whether V_i' and $h(ID_i' \| T_i' \| J_i')$ are equal. If they are not equal, S stops the request; otherwise, S generates a new pseudo identity pid_i^{new}, computes $I_i^{new} = h(x \| pid_i^{new})$, $V_s = h(ID_i' \| T_i' \| V_i' \| pid_i^{new} \| I_i^{new} \| T_s)$, $C_2 = E_{I_i}(V_s \| T_s \| pid_i^{new} \| I_i^{new})$, $sk = h(J_i' \| T_i' \| T_s \| ID_i')$ and sends the message $m_2 = \{C_2\}$ to U_i, where T_s is the timestamp generated by S.

2) After receiving $m_2=\{C_2\}$, U_i computes $(V_s'\|T_s'\|pid_i^{new}\|I_i^{new})=D_{I_i}(C_2)$ and checks whether T_s' is fresh. If it is not fresh, U_i stops the session; otherwise, U_i checks whether the equation $V_s'=h(ID_i\|T_i\|V_i\|pid_i^{new}\|I_i^{new}\|T_s)$ holds. If it does not hold, U_i stops the session; otherwise, U_i replaces pid_i and E_i with pid_i^{new} and $I_i^{new}\oplus h(RPW_i\|ID_i)$ separately. At last, U_i computes the session key $sk=h(J_i\|T_i\|T_s'\|ID_i)$.

4.4. Password Change Phase

When U_i wants to change his password, he inserts his smart card into a card reader and inputs his identity ID_i, the old password PW_i and a new password PW_i^{new}. Then step 2) of the login phase and step 1) of the authentication phase are executed.

After receiving $m_2=\{C_2\}$, U_i computes $(V_s'\|T_s'\|pid_i^{new}\|I_i^{new})=D_{I_i}(C_2)$ and checks whether T_s' is fresh. If it is not fresh, U_i stops the session; otherwise, U_i checks whether the equation $V_s'=h(ID_i\|T_i\|V_i\|pid_i^{new}\|I_i^{new}\|T_s)$ holds. If it does not hold, U_i stops the session; otherwise, U_i computes $HPW_i^{new}=h(r_i\|PW_i^{new})$, $L_i^{new}=L_i\oplus RPW_i\oplus RPW_i^{new}$, $E_i^{new}=I_i^{new}\oplus h(RPW_i^{new}\|ID_i)$ and replaces L_i and E_i with L_i^{new} and E_i^{new} separately.

4.5. Lost Smart Card Revocation Phase

When U_i loses his smart card, he can re-register at S through the secure channel as the registration phase. S verifies U_i , makes $N=N+1$ and stores (ID_i,N) into the account table. At last, S issues a new smart card to U_i.

5. Security Analysis

In this section, we will analyze the security of our scheme. We will show our scheme could withstand general attacks and provide common security features.

5.1. User Anonymity

The user's identity ID_i is included in the ciphertext $C_1=E_{I_i}(ID_i\|T_i\|V_i)$, where $V_i=h(ID_i\|T_i\|J_i)$, $I_i=h(x\|pid_i)$ and T_i is the timestamp generated by U_i. Without the knowledge of the server's secret key x, the adversary, including the malicious user, cannot compute I_i and decrypt C_1. Therefore, our scheme could provide the user anonymity.

5.2. Mutual Authentication

Without the knowledge $J_i=h(x\|ID_i\|N)$, any adversary including the malicious user cannot generate $V_i=h(ID_i\|T_i\|J_i)$. Then, he cannot generate a legal message $m_1=\{pid_i,C_1\}$, where $C_1=E_{I_i}(ID_i\|T_i\|V_i)$ and T_i is the timestamp generated by U_i. Therefore, S could authenticate U_i by checking whether V_i' and $h(ID_i'\|T_i'\|J_i')$ are equal in Step 1) of the authentication scheme.

Without the knowledge the server's secret key x, any adversary including malicious cannot compute $I_i=h(x\|pid_i)$ and get $(ID_i'\|T_i'\|V_i')$ by decrypting C_1. Then, he cannot generate a legal message $m_2=\{C_2\}$, where $C_2=E_{I_i}(V_s\|T_s\|pid_i^{new}\|I_i^{new})$, $V_s=h(ID_i'\|T_i'\|V_i'\|pid_i^{new}\|I_i^{new}\|T_s)$ and T_s is the timestamp generated by S. Therefore, U_i could authenticate S by checking whether the equation $V_s'=h(ID_i\|T_i\|V_i\|pid_i^{new}\|I_i^{new}\|T_s)$ holds in Step 2) of the authentication phase.

5.3. Privileged Insider Attack

In the registration phase of our scheme, the user U_i sends the message $\{ID_i, HPW_i\}$ to the sever, where $HPW_i = h(r_i \| PW_i)$ and r_i is a random number generate by U_i. Then, the privileged insider of the server cannot get U_i's password PW_i since it is protected by the secure hash function and the random number. Therefore, our scheme could withstand the privileged insider attack.

5.4. Man-in-the-middle Attack

From the analysis in Section 5.2, we know that our scheme could provide mutual authentication between the user and the server. Therefore, our scheme could withstand the man-in-the-middle attack.

5.5. Replay Attack

The adversary may intercept the message $m_1 = \{pid_i, C_1\}$ and replay it to the server, where $HPW_i = h(r_i \| PW_i)$, $J_i = L_i \oplus RPW_i$, $I_i = E_i \oplus h(RPW_i \| ID_i)$, $V_i = h(ID_i \| T_i \| J_i)$, $C_1 = E_{I_i}(ID_i \| T_i \| V_i)$ and T_i is the timestamp generated by U_i. In the Step 1) of the authentication, the server will check the freshness of T_i, then he could find the attack easily.

The adversary may intercept the message $m_2 = \{C_2\}$ and replay it to the user, where $C_2 = E_{I_i}(V_s \| T_s \| pid_i^{new} \| I_i^{new})$, $V_s = h(ID_i' \| T_i' \| V_i' \| pid_i^{new} \| I_i^{new} \| T_s)$ and T_s is the timestamp generated by S. In the Step 2) of the authentication phase, the user will check the freshness of T_s, then he could find the attack easily.

5.6. Impersonation Attack

To impersonation the user to the server, the adversary has to generate a legal message $m_1 = \{pid_i, C_1\}$, where $C_1 = E_{I_i}(ID_i \| T_i \| V_i)$, $V_i = h(ID_i \| T_i \| J_i)$ and T_i is the current timestamp. However, any adversary including the malicious user cannot generate V_i if he does not know the value of $J_i = h(x \| ID_i \| N)$. Therefore, our scheme could withstand the impersonation attack.

5.7. Server Spoofing Attack

To impersonate the serve to the user, the adversary has to generate a legal message $m_2 = \{C_2\}$ when he intercepts the message $m_1 = \{pid_i, C_1\}$, where $C_1 = E_{I_i}(ID_i \| T_i \| V_i)$, $V_i = h(ID_i \| T_i \| J_i)$, $C_2 = E_{I_i}(V_s \| T_s \| pid_i^{new} \| I_i^{new})$, $V_s = h(ID_i' \| T_i' \| V_i' \| pid_i^{new} \| I_i^{new} \| T_s)$. However, any adversary including malicious cannot compute $I_i = h(x \| pid_i)$ and get $(ID_i' \| T_i' \| V_i')$ by decrypting C_1 if he does not know the server's secret key x. Therefore, our scheme could withstand the server spoofing attack.

5.8. Stolen Verifier Attack

In our scheme, the server just maintains a table of tuple (ID_i, N) and there is no user's password is stored in the table. Therefore, our scheme could withstand the stolen verifier attack.

5.9. Modification Attack

The adversary may intercept the message $m_1 = \{pid_i, C_1\}$ and resend it after modifying it at his will. However, the user could find the attack by checking whether V_i' and $h(ID_i' \| T_i' \| J_i')$ are equal. By the similar method, we could show the user could find the modification of $m_2 = \{C_2\}$. Therefore, our scheme could withstand the modification attack.

5.10. Stolen Smart Card Attack

The adversary may steal the user's smart card and extract the stored information $\{pid_i, L_i, E_i\}$ through the side channel attack, where $I_i = h(x \| pid_i)$, $J_i = h(x \| ID_i \| N)$, $E_i = I_i \oplus h(RPW_i \| ID_i)$ and $L_i = J_i \oplus RPW_i$. However, there is no message related pid_i and E_i could be found since the user will change pid_i and E_i in every session. Therefore, he cannot verify whether his guess is correct and our scheme could withstand the stolen smart card attack.

6. Performance Analysis

In this section, we will analyze the performance of our scheme. To the best of our knowledge, Jiang et al.'s scheme [20] and Wu and Xu's scheme [21] are more suitable for TMIS than other schemes. We will also compare our scheme with that two schemes. For convenience, some notations are defined as follows.

a) T_H : the running time of a hash function operation;

b) T_S : the running time of a symmetric encryption/decryption operation;

c) T_{XOR} : the running time of a bitwise XOR operation;

We just need to compare the performance in the login and authentication phase of different schemes since other phases are executed only one time. The performance comparisons are listed in Table 1.

Table 1

	Jiang et al.'s scheme	Wu and Xu's scheme	Our scheme
User	$3T_H + 1T_S + 1T_{XOR}$	$6T_H + 2T_S + 5T_{XOR}$	$5T_H + 2T_S + 3T_{XOR}$
Server	$3T_H + 3T_S$	$5T_H + 2T_S + 3T_{XOR}$	$5T_H + 2T_S$
Total	$6T_H + 4T_S + 1T_{XOR}$	$11T_H + 4T_S + 8T_{XOR}$	$10T_H + 4T_S + 5T_{XOR}$

In the login and authentication phase of Jiang et al.'s scheme [20], $3T_H + 1T_S + 1T_{XOR}$ and $3T_H + 3T_S$ are needed at the side of user and server separately. In the login and authentication phase of Wu and Xu's scheme [21], $6T_H + 2T_S + 5T_{XOR}$ and $5T_H + 2T_S + 3T_{XOR}$ are needed at the side of user and server separately. In the login and authentication phase of our scheme, $5T_H + 2T_S + 3T_{XOR}$ and $5T_H + 2T_S$ are needed at the side of user and server separately. Besides, the running time of a bitwise XOR operation could be ignored when compared with that of a hash function or a symmetric encryption/decryption operation. Therefore, Jiang et al.'s scheme has better performance than Wu and Xu's scheme and our scheme. However, Wu and Xu pointed out that Jiang et al.'s scheme has useless identity and is vulnerable to off-line password guessing attack, user impersonation attack and DoS attack. Therefore, Jiang et al.'s scheme is not suitable for practical applications. We have demonstrated that Wu and Xu et al.'s scheme is venerable to the server spoofing attack and cannot provide user anonymity. Besides, our scheme has better performance than Wu and Xu et al.'s scheme. Therefore, we could conclude that our scheme is more suitable for TIMS.

7. Conclusion

In this paper, we demonstrate that Wu and Xu's scheme cannot withstand the server spoofing attack and cannot provide the user anonymity. To overcome those weaknesses, we proposed an improved authentication scheme for TMIS. Security analysis shows our scheme could withstand general attacks and overcome the drawback of Wu and Xu's scheme. Performance analysis shows our scheme also has better performance than Wu and Xu's scheme. Therefore, we could conclude that our scheme is more suitable for TMIS.

Acknowledgements

The authors would like to thank the anonymous referees for their invaluable comments. This research was supported by National Natural Science Foundation of China (no.61202447), the Natural Science Foundation of Hebei Province of China (no. F2013501066) and the Northeastern University at Qinhuangdao Science and Technology Support Program (no. xnk201307).

References

[1] Lamport L. Password authentication with insecure communication. *Commun ACM* 24:28–30, 1981.
[2] Hwang MS, Li LH. A new remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron*. 2000; 46(1): 28–30.
[3] He D, Chen J, Hu J. Further improvement of Juang et al.'s password-authenticated key agreement scheme using smart cards. *Kuwait Journal of Science & Engineering.* 2011; 38(2A): 55-68.
[4] He D, Chen J, Chen Y. A secure mutual authentication scheme for session initiation scheme using elliptic curve cryptography. *Security and Communication Networks.* 2012; 5(12): 1423–1429.
[5] He D, Chen Y, Chen J. Cryptanalysis and improvement of an extended chaotic maps-based key agreement scheme. *Nonlinear Dynamics.* 2012; 69(3): 1149–1157.
[6] He D, Chen J, Hu J. Improvement on a smart card based password authentication scheme. *Journal of Internet Technology* 2012; 13(3): 405–410.
[7] He D. An efficient remote user authentication and key exchange scheme for mobile client–server environment from pairings. *Ad Hoc Networks* 2012; 10(6): 1009–1016.
[8] He D, Chen J, Hu J. An ID-based client authentication with key agreement scheme for mobile client–server environment on ECC with provable security. *Information Fusion.* 2012; 13(3): 223-230.
[9] He D, Wang D, Wu S. Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards. *Information Technology and Control.* 2013; 42(2): 170-177.
[10] He D, Zhang Y, Chen J. Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks. *Wireless Personal Communications*, DOI: 10.1007/s11277-013-1282-x
[11] Wu ZY, Lee YC, Lai F, Lee HC, Chung Y. A secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems.* 2012; 36: 1529–35.
[12] He DB, Chen JH, Zhang R. A more secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems.*2012; 36:1989–1995.
[13] Wei J, Hu X, Liu W. An improved authentication scheme for telecare medicine information systems. *Journal of Medical Systems.* 2012; 36(6): 3597–3604.
[14] Zhu Z. An efficient authentication scheme for telecare medicine information systems. *Journal of Medical Systems.* 2012; 36(6): 3833–3838.
[15] Das ML, Saxena A, Gulati VP. A dynamic id-based remote user authentication scheme. *IEEE Trans. Consum. Electron*., 2004; 50(2): 629–631.
[16] Chen HM, Lo JW, Yeh CK. An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. *Journal of Medical Systems.* 2012; 36(6): 3907–3915.
[17] Cao T, Zhai J. Improved dynamic id-based authentication scheme for telecare medical information systems. *Journal of Medical Systems*. 2013. doi:1007/s10916-012-9912-5.
[18] Xie Q, Zhang J, Dong N. Robust anonymous authentication scheme for telecare medical information systems. *Journal of Medical Systems*, 2013. doi:10.1007/s10916-012-9911-6.
[19] Lin HY. On the security of a dynamic id-based authentication scheme for telecare medical information systems. *Journal of Medical Systems*. 2013. doi:10.1007/s10916-013-9929-4.
[20] Jiang Q, Ma J, Ma Z, Li G. A privacy enhanced authentication scheme for telecare medical information systems. *Journal of Medical Systems*. 2013. doi:10.1007/s10916-012-9897-0.
[21] Wu F, Xu L. Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. *Journal of Medical Systems*. 2013. doi: 10.1007/s10916-013-9958-z.