Journal of Medical Systems

Improvement of a Uniqueness-and-Anonymity-Preserving User Authentication Scheme for Connected Health Care

--Manuscript Draft--

Manuscript Number:	JOMS-D-14-00178
Full Title:	Improvement of a Uniqueness-and-Anonymity-Preserving User Authentication Scheme for Connected Health Care
Article Type:	Research Paper
Section/Category:	Mobile Systems
Keywords:	Connected health care; Authentication; Anonymity; Biometrics; Smart card
Abstract:	Patient's privacy-preserving, security and mutual authentication between patient and the medical server are the important mechanism in connected health care applications, such as telecare medical information systems and personally controlled health records systems. In 2013, Wen showed that Das et al.'s scheme is vulnerable to the replay attack, user impersonation attacks and off-line guessing attacks, and then proposed an improved scheme using biometrics, password and smart card to overcome these weaknesses. However, we show that Wen's scheme is still vulnerable to off-line password guessing attacks, does not provide user's anonymity and perfect forward secrecy. Further, we propose an improved scheme to fix these weaknesses, and use the applied pi calculus based formal verification tool ProVerif to prove the security and authentication.

Improvement of a Uniqueness-and-Anonymity-Preserving User Authentication Scheme for Connected Health Care

Qi Xie[1*], Wenhao Liu[1], Shengbao Wang[1], Lidong Han[1], Bin Hu[1], Ting Wu[2]

1. Hangzhou Key Laboratory of Cryptography and Network Security, Hangzhou Normal University, China

*E-mail: qixie68@126.com

2. School of Computer Science, Hangzhou Dianzi University, China

Abstract: Patient's privacy-preserving, security and mutual authentication between patient and the medical server are the important mechanism in connected health care applications, such as telecare medical information systems and personally controlled health records systems. In 2013, Wen showed that Das et al.'s scheme is vulnerable to the replay attack, user impersonation attacks and off-line guessing attacks, and then proposed an improved scheme using biometrics, password and smart card to overcome these weaknesses. However, we show that Wen's scheme is still vulnerable to off-line password guessing attacks, does not provide user's anonymity and perfect forward secrecy. Further, we propose an improved scheme to fix these weaknesses, and use the applied pi calculus based formal verification tool ProVerif to prove the security and authentication.

Keywords: Connected health care. Authentication. Anonymity. Biometrics. Smart card.

1. Introduction

The traditional medical records mode is changing due to the rapid development of computer and communication technology. Telecare medical information systems (TMIS) and personally controlled health records systems, the applications of connected health care, have attracted much attention. Take TMIS as example, it maintains the patients' diagnostic records, when a doctor wants to know one patient's anamnesis, he can easily access to TMIS and diagnose quickly, and the repeated physical examination is not needed. TMIS can save the patients' expenses and time. In order to prevent medical records from being damaged or accessed by illegal users, authentication scheme with patient's anonymity-preserving plays an important role in connected health care applications [1,2]. However, some recently proposed user authentication schemes for TMIS can not achieve patient's anonymity [3-7].

In order to provide user's anonymity against an adversary knows user's identity from the authentication process, Das et al. [8] proposed a dynamic ID-based password authentication scheme. But Awashti [9] and Ku-Chang [10] showed that Das et al.'s scheme is vulnerable to password guessing attack and impersonation attack, and can not provide user's anonymity. After that, Wang et al. [11] proposed another improved scheme, but Khan et al. [12] showed that their scheme can not provide user's anonymity and proposed a further improved scheme. Unfortunately, Chen et al. [13] showed that Khan et al.'s scheme can not achieve the user's anonymity and proposed a new dynamic ID-based password authentication scheme using smart card. In 2013, Xie et al. [14] showed that Chen et al.'s scheme does not provide user privacy protection and perfect forward secrecy, is vulnerable to off-line password guessing attack and impersonation attack once an adversary can know all information stored in smart card.

All above mentioned schemes are based on smart card and password, the security is only based on the password. In 2013, Chang et al. [15] proposed a uniqueness-and-anonymity-preserving user authentication scheme for connected health care using biometric, password and smart card. The advantages of using biometric (e.g. irises) are that it can not be guessed, forged, lost and forgotten, and is difficult to copy. Unfortunately, Das et al. [16] showed that their scheme has some weaknesses, such as, is vulnerable to privileged insider attack and man-in-the middle attack, and proposed an improved scheme. Wen [17] showed that Das et al.'s scheme is insecure against the replay attack, user impersonation attacks and off-line guessing attacks, and presented the further improved scheme. Very recently, Tsai et al. [18] and Tan [19] also proposed biometric, password and smart card based user anonymous authentication schemes.

In this paper, we show that a uniqueness-and-anonymity-preserving user authentication scheme for connected health care proposed by Wen [17] does not provide user anonymity and perfect forward secrecy, is vulnerable to off-line password guessing attack. Then we propose a new scheme to solve their security weaknesses.

The rest of the paper is organized as follows. In Sections 2 and 3, we review and cryptanalysis of Wen's scheme. An improved scheme is proposed in Section 4. After that, we present security analysis and formal verification in Sections 5 and 6. In Section 7, we present the performance evaluation, and conclude the paper in Section 8.

2. Review of Wen's Scheme

In this section, we only review the first two phases of Wen's scheme, which consists of registration, login and verification, password change phases. The following notation will be used in this paper:

U_i : The user

ID_i : U_i 's identity.

PW_i : U_i 's password.

S_j : A trustworthy server.

B_i : Personal biometrics of U_i .

C_i : Smart card of U_i .

X_s :Secret key of S_j .

K :Secret number of U_i .

NID_i : A random identity chosen by S_j for U_i .

$h(\cdot)$: A secure collision-free one-way hash function.

$H(\cdot)$:BioHashing.

$\oplus$:The bitwise XOR operation.

$||$:The concatenation operation.

$E_k() / D_k()$: The symmetric encryption and decryption algorithms with key k .

2.1 Registration phase

In registration phase, U_i and S_j perform the following steps:

Step 1: U_i chooses a random number K, his identity ID_i , password PW_i and enters his biometrics B_i on a specific device, and computes

$$f_i = H(ID_i \,||\, PW_i \,||\, B_i), RPW_i = h(ID_i \,||\, K \,||\, PW_i) .$$

Then he sends $\{ID_i, f_i, RPW_i\}$ to S_j via a secure channel.

Step 2: After receiving the message $\{ID_i, f_i, RPW_i\}$ from U_i , S_j chooses a random identity NID_i for U_i and computes

$$e_i = h(ID_i \,||\, X_s) \oplus h(RPW_i \,||\, f_i), \; TD_i = NID_i \oplus h(ID_i \,||\, RPWi), \; D_i = TD_i ,$$

where X_s is a secret key of S_j . S_j generates a counter $ctr_{U_i} = 0$ and creates a record (ID_i, NID_i, ctr_{Ui}) for U_i in its database.

Step 3: S_j issues a smart card C_i to U_i via a secure channel, which contains $\{TD_i, D_i, h(\cdot), H(\cdot), ctr_{U_i}, f_i, e_i\}$.

After receiving the smart card C_i, U_i stores K in the smart card.

2.2 Login and authentication phase

When a legal user U_i wants to login S_j, they need perform the following steps. In order to resist DoS attack, Wen's scheme has two cases according to whether the latest identities kept by C_i and S_j are matched or not.

Step 1: U_i inserts his smart card C_i into a card reader, and inputs his biometrics B_i, ID_i, PW_i, C_i computes $H(ID_i \| PW_i \| B_i)$ and verifies whether it equals to f_i or not. If not, terminates. Otherwise, U_i executes the following two cases.

Case I: the latest identities kept by C_i and S_j are matched.

Step 2: C_i selects a random nonce R_c and computes

$$RPW_i = h(ID_i \| K \| PW_i),$$

$$NID_i^{'} = h(ID_i \| RPW_i) \oplus D_i,$$

$$M_1 = e_i \oplus h(RPW_i \| f_i) = h(ID_i \| X_s),$$

$$M_2 = E_{M_1}(R_c),$$

$$ctr'_{U_i} = ctr_{U_i} + 1,$$

$$M_3 = h(ID_i \| R_c \| ctr'_{U_i}).$$

Then, C_i sends $\{ctr'_{U_i}, NID_i^{'}, M_2, M_3\}$ to S_j.

Step 3: After receiving $\{ctr'_{U_i}, NID_i^{'}, M_2, M_3\}$ from U_i, S_j checks the format of NID_i and finds the NID_i, ID_i and ctr_{U_i} in the database. If NID_i is found, does Step 4; Otherwise, S_j does the Step7 in Case II.

Step 4: S_j computes $M_4 = h(ID_i \| X_s)$, $M_5 = D_{M_4}(M_2) = R_c$ and $ctr'_{U_i} = ctr_{U_i} + 1$, and then verifies if $h(ID_i \| M_5 \| ctr'_{U_i}) = M_3$ and $ctr_{U_i}^{'} > ctr_{U_i}$. If not, S_j rejects it. Otherwise, S_j chooses a random nonce R_s and NID_i^{new}, computes $M_6 = E_{M_4}(R_s)$, $M_7 = h(R_s \| M_5) \oplus NID_i^{new} = h(R_s \| R_c) \oplus NID_i^{new}$, $M_8 = h(M_4 \| M_5 \| R_s \| ID_i \| NID_i^{new})$, and sends $\{M_6, M_7, M_8\}$ to C_i.

Step 5: C_i computes $M_9 = D_{M_1}(M_6) = R_s$, $NID_i^{new} = M_7 \oplus h(M_9 \| R_c)$, and verifies whether $M_8 = h(M_1 \| R_c \| M_9 \| ID_i \| NID_i^{new})$ or not. If not, terminates. Otherwise, C_i updates TD_i and D_i with D_i and $D_i \oplus NID_i^{'} \oplus NID_i^{new}$, respectively. Then C_i computes and sends $M_{10} = h((M_9+1) \| ID_i \| NID_i^{new} \| (R_c+1))$ to S_j. C_i also computes the session key $SK_{U_i,S_j} = h(ID_i \| R_c \| M_9 \| M_2 \| M_1)$.

Step 6: S_j computes $h((R_s+1) \| ID_i \| NID_i^{new} \| (M_5+1))$ and checks if it equals to M_{10}. If not, terminates. Otherwise, S_j updates (NID_i, ctr_{U_i}) with $(NID_i^{new}, ctr_{U_i}+1)$ in its database and S_j computes the session key $SK_{U_i,S_j} = h(ID_i \| M_5 \| R_s \| M_2 \| M_4)$.

Thus, both U_i and S_j share the same session key

$$SK_{U_i,S_j} = h(ID_i \| R_c \| R_s \| M_2 \| h(ID_i \| X_s)).$$

Case II: the latest random identities kept by C_i and S_j are distinct.

Step 7: All steps in this case are almost the same as those in **Case I** except $NID_i^{'} = h(ID_i \| RPW_i) \oplus TD_i$ in Step2, and C_i needs to update D_i with $D_i \oplus NID_i^{'} \oplus NID_i^{new}$ without changing TD_i in Step5.

3. Weaknesses of Wen's Scheme

In this section, we show that Wen's scheme has some weaknesses, the details are as follows.

3.1 Off-line password guessing attack

Wen claimed that their scheme can resist off-line password guessing attack even if an adversary can know all information $\{TD_i, D_i, h(\cdot), H(\cdot), ctr_{U_i}, f_i, e_i, K\}$ stored in smart card. However, the adversary can get the transmitted messages $\left\{ctr_{U_i}^{'}, NID_i^{'}, M_2, M_3\right\}$ in public channel, and can guess $\{ID_i', PW_i'\}$ and compute $RPW_i' = h(ID_i' \| K \| PW_i')$, thus the adversary can check if $TD_i \oplus h(ID_i' \| RPW_i') = NID_i'$. If yes, the guessed $\{ID_i', PW_i'\}$ are correct. Otherwise, the adversary can guess another identity and password and tries again. Since the identity and password is short and easy to remember, in particular, the adversary can easy to obtain the user's identity as an insider attacker, therefore, this attack is valid.

On the other hand, the adversary can also compute

$M_1' = (h(ID_i \| X_s))' = e_i \oplus h(RPW_i' \| f_i)$,

$(R_c)' = D_{M_1'}(M_2)$,

and can also check if $M_3 = h(ID_i' \| R_c' \| ctr'_{U_i})$. If yes, the guessed $\{ID_i', PW_i'\}$ are correct. Otherwise, the adversary guesses another identity and password and tries again.

Therefore, Wen's scheme is vulnerable to off-line password guessing attacks. Thus, the adversary can impersonate the user easily.

3.2 Lack of perfect forward secrecy

In Wen's scheme, the session key is $SK_{U_i,S_j} = h(ID_i \| R_c \| R_s \| M_2 \| h(ID_i \| X_s))$. Therefore, if an adversary can know all long-term secret information, e.g., the server's secret key X_s and user's identity ID_i, and can get all transmitted messages $\{ctr'_{U_i}, NID'_i, M_2, M_3\}$, $\{M_6, M_7, M_8\}$ in public channel, then he can compute $M_1 = h(ID_i \| X_s)$, $R_c = D_{M_1}(M_2)$, $R_s = D_{M_1}(M_6)$. Thus, the adversary can know the session key $SK_{U_i,S_j} = h(ID_i \| R_c \| R_s \| M_2 \| h(ID_i \| X_s))$, and can know all transmitted messages encrypted by SK_{U_i,S_j}.

3.3 Lack of user's anonymity

Wen claimed that his scheme can achieve U_i's anonymity by using the random identity NID_i. However, Since (ID_i, NID_i, ctr_{Ui}) are stored in account table in plaintext. Therefore, if an adversary can access to account table (or steal the account table), and have obtained the login message $\{ctr'_{U_i}, NID'_i, M_2, M_3\}$ from the public network. Then, the adversary can lookup ID_i in account table and can know the U_i's identity.

4. The Proposed Scheme

The proposed scheme also consists of three phases: registration, login and verification, password change phases. Let $h()$ be a one-way collision resistant cryptographic hash function which maps to an integer, E be an elliptic curve defined over a finite field with large order n and P be a generator on E with large order n.The details of our scheme are as follows.

4.1 Registration

In this phase, the patient U_i and the medical server S_j perform the following steps.

Step 1: U_i chooses his identity ID_i and password PW_i, scans and enters his personal biometrics B_i. It is worth mentioning that no one can get B_i except U_i, and the biometrics scanner can be combined in the smart card reader. Then U_i computes $RPW_i = h(B_i \| ID_i \| PW_i)$ and $f_i = h(RPW_i)$, and sends ID_i to S_j via a secure channel.

Step 2: After receiving the message ID_i, S_j checks the validity of ID_i and chooses a random identity NID_{ij} and computes $e_i = h(ID_i \| X_s)$, where X_s is a secret number kept by S_j. S_j computes $y_i = E_{X_s}(ID_i, ctr_{U_i})$ for U_i and creates a record (NID_{ij}, y_i) in its database, where $ctr_{U_i} = 0$.

Step 3: Finally, S_j stores $\{NID_{ij}, P, h(\cdot), ctr_{U_i}, e_i\}$ into a smart card and sends it to U_i via a secure channel.

Step 4: After receiving the smart card, U_i computes

$$TID_i = RPW_i \oplus e_i = h(B_i \| ID_i \| PW_i) \oplus h(ID_i \| X_s),$$

and stores f_i into the smart card, change e_i with TID_i. That is, the smart card contains $\{NID_{ij}, P, h(\cdot), ctr_{U_i}, f_i, TID_i\}$.

4.2 Login and Verification

When U_i wants to logon to the TMIS system, he inserts his smart card into a device, inputs his ID_i, password PW_i and biometrics B_i, then the smart card performs the following steps. Figure 1 illustrates this phase.

Step 1: Smart card computes $RPW_i = h(B_i \| ID_i \| PW_i)$ and checks if $f_i = h(RPW_i)$. If not, U_i inputs his ID_i, password PW_i and biometrics B_i again. Otherwise, it generates a random number a, computes

$$e_i = RPW_i \oplus TID_i = h(ID_i \| X_s),$$
$$r_1 = aP,$$
$$ctr'_{U_i} = ctr_{U_i} + 1$$
$$M_1 = E_{e_i}(r_1 \| ctr'_{U_i}),$$
$$M_2 = h(ID_i \| r_1 \| ctr'_{U_i} \| NID_{ij}).$$

Then, smart card sends $\{M_1, M_2, ctr'_{U_i}, NID_{ij}\}$ to S_j.

Step 2: After receiving the message $\{M_1, M_2, ctr'_{U_i}, NID_{ij}\}$, S_j checks NID_{ij} in database and finds y_i, computes

$$D_{X_s}(y_i) = \{ID_i, ctr_{U_i}\},$$

$h(ID_i \| X_s)$,

$D_{h(ID_i \| Xs)}(M_1) = \{r_1, ctr'_{U_i}\}$,

and checks if $ctr'_{U_i} > ctr_{U_i}$. If not, terminates it. Otherwise, S_j computes $h(ID_i \| r_1 \| ctr'_{Ui} \| NID_{ij})$ and checks if it equals to M_2. If not, rejects it. Otherwise, S_j generates a random number b, a random identity NID_{ij}', and computes

$r_2 = bP$,

$r = br_1 = baP$,

$M_3 = h(r_1 \| r) \oplus NID_{ij}'$

$M_4 = h(r_2 \| r_1 \| r \| NID_{ij}')$

Then, S_j sends $\{M_3, M_4, r_2\}$ to U_i.

Step 3: When U_i receives $\{M_3, M_4, r_2\}$, he computes

$$r = ar_2 = baP,\ NID_{ij}' = h(r_1 \| r) \oplus M_3,$$

and $h(r_2 \| r_1 \| r \| NID_{ij}')$, then checks if $h(r_2 \| r_1 \| r \| NID_{ij}')$ equals to M_4. If not, terminates it. Otherwise, he computes $M_5 = h(NID_{ij}' \| r)$ and the session key $SK = h(r_2 \| r_1 \| r \| ctr'_{Ui})$, updates (NID_{ij}, ctr_{U_i}) with (NID_{ij}', ctr'_{U_i}) in smart card. Finally, U_i sends M_5 to S_j.

Step 4: After receiving the message M_5, S_j checks the validity of M_5, if not, S_j sends $M_6 = E_{h(ID_i \| Xs)}(M_5\ \textit{is not correct})$ and terminates it. Otherwise, S_j computes the session key $SK = h(r_2 \| r_1 \| r \| ctr'_{Ui})$, $y_i' = E_{X_s}(ID_i, ctr'_{U_i})$ and updates the record (NID_{ij}, y_i') of U_i, where $NID_{ij} = NID_{ij}'$.

If U_i receives M_6, he has to re-authenticate with S_j and does not update (NID_{ij}, ctr_{U_i}) in his smart card.

4.3 Password change

When U_i wants to change his password, he inserts his smart card into a device, inputs his old password PW_i and new password PW_i^{new}, his ID_i and B_i, then the smart card first checks the correctness of $RPW_i = h(B_i \| ID_i \| PW_i)$ by $f_i = h(RPW_i)$, then computes

$e_i = RPW_i \oplus TID_i = h(ID_i \| X_s)$,

$RPW_i^{new} = h(B_i \| ID_i \| PW_i^{new})$,

$f_i^{new} = h(RPW_i^{new})$,

$TID_i^{new} = RPW_i^{new} \oplus e_i = h(B_i \| ID_i \| PW_i^{new}) \oplus h(ID_i \| X_s)$, and updates f_i and TID_i with f_i^{new} and TID_i^{new}.

Fig. 1 Login and authentication phase of the proposed scheme.

U		S
$RPW_i = h(B_i \parallel ID_i \parallel PW_i)$ $f_i \stackrel{?}{=} h(RPW_i)$ $e_i = RPW_i \oplus TID_i = h(ID_i \parallel X_s)$ $r_1 = aP$ $ctr'_{U_i} = ctr_{U_i} + 1$ $M_1 = E_{e_i}(r_1 \parallel ctr'_{U_i})$ $M_2 = h(ID_i \parallel r_1 \parallel ctr'_{U_i} \parallel NID_{ij})$		
	$\xrightarrow{\{M_1, M_2, ctr'_{U_i}, NID_{ij}\}}$	
		Check NID_{ij}, find y_i $D_{X_s}(y_i) = \{ID_i, ctr_{U_i}\}$ $h(ID_i \parallel X_s)$ $D_{h(ID_i \parallel X_s)}(M_1) = \{r_1, ctr'_{U_i}\}$ check $ctr'_{U_i} > ctr_{U_i}$ $h(ID_i \parallel r_1 \parallel ctr'_{U_i} \parallel NID_{ij}) \stackrel{?}{=} M_2$ $r_2 = bP, r = br_1 = baP$ $M_3 = h(r_1 \parallel r) \oplus NID_{ij}'$ $M_4 = h(r_2 \parallel r_1 \parallel r \parallel NID_{ij}')$
	$\xleftarrow{\{M_3, M_4, r_2\}}$	
$r = ar_2 = baP$ $NID_{ij}' = h(r_1 \parallel r) \oplus M_3$ $h(r_2 \parallel r_1 \parallel r \parallel NID_{ij}') \stackrel{?}{=} M_4$ $M_5 = h(NID_{ij}' \parallel r)$ $SK = h(r_2 \parallel r_1 \parallel r \parallel ctr'_{U_i})$		
	$\xrightarrow{M_5}$	
		Verify M_4 $SK = h(r_2 \parallel r_1 \parallel r \parallel ctr'_{U_i})$
The session key is $SK = h(r_2 \parallel r_1 \parallel r \parallel ctr'_{U_i})$		

5. Security Analysis

In this section, we show that the proposed scheme can resist various attacks.

5.1 Patient's privacy protection

If an adversary can get all information $\{NID_{ij}, P, h(\cdot), ctr_{U_i}, f_i, TID_i\}$ stored in smart card, and all transmitted messages $\{M_1, M_2, ctr'_{U_i}, NID_{ij}\}$, $\{M_3, M_4, r_2\}$ and M_5 in public channel, and he wants to know the patient U_i's identity ID_i. Since the adversary can not know U_i's biometrics B_i, so he can not know ID_i by guessing $\{ID_i, PW_i, B_i\}$ and checking whether $f_i = h(h(B_i \| ID_i \| PW_i))$ or not.

On the other hand, the adversary can not identify ID_i from $M_2 = h(ID_i \| r_1 \| ctr'_{U_i} \| NID_{ij})$ and $y_i = E_{X_s}(ID_i, ctr_{U_i})$ without knowing r_1 and the medical server S_j's secret key X_s, even if he can get account table in server's database, as we know, the random identity of U_i is changed in each session run.

Therefore, our scheme provides patient's anonymity and untraceability.

5.2 Off-line password guessing attack

If an adversary can get all information $\{NID_{ij}, P, h(\cdot), ctr_{U_i}, f_i, TID_i\}$ stored in smart card, and all transmitted messages $\{M_1, M_2, ctr'_{U_i}, NID_{ij}\}$, $\{M_3, M_4, r_2\}$ and M_5 in public channel, and he wants to launch off-line password guessing attack. However, the adversary can not compute $RPW_i = h(B_i \| ID_i \| PW_i)$ for guessed ID_i and password PW_i without knowing U_i's biometrics B_i, and can not check if $f_i = h(RPW_i)$. On the other hand, the transmitted messages do not conducive to the adversary to guess the password because he can not compute RPW_i.

So our scheme can resist off-line password guessing attack.

5.3 Replay attacks

If an adversary replays $\{M_1, M_2, ctr'_{U_i}, NID_{ij}\}$ to S_j, S_j will detect that $ctr'_{U_i} > ctr_{U_i}$ is not hold; if the adversary changes ctr'_{U_i} to $ctr'_{U_i}+1$, then $M_2 = h(ID_i \| r_1 \| ctr'_{U_i} \| NID_{ij})$ will not hold.

If an adversary replays $\{M_3, M_4, r_2\}$ to U_i, U_i will find that $M_4 = h(r_2 \| r_1 \| r \| NID_{ij}')$ will not hold because r_1 is changed in each session run.

5.4 Impersonation attacks

If an adversary gets all information stored in smart card and all transmitted messages in public channel, and impersonates the patient to pass through the authentication process of S_j. Because he does not know the U_i 's biometrics B_i and can not compute RPW_i from $f_i = h(RPW_i)$, so he can not know $e_i = RPW_i \oplus TID_i = h(ID_i \| X_s)$ and compute $M_1' = E_{e_i}(r_1' \| ctr'_{U_i})$, where $r_1' = a'P$ for randomly chosen a'. Therefore, the login message $\{M_1', M_2', ctr'_{U_i}, NID_{ij}\}$ will not pass the authentication process of S_j, where $M_2' = h(ID_i \| r_1' \| ctr'_{U_i} \| NID_{ij})$.

If an adversary wants to impersonate the medical server S_j, however, he can not decrypt M_1 to obtain r_1 without knowing S_j 's secret key X_s, and can not compute $r = br_1 = baP$, and the valid $M_4 = h(r_2 \| r_1 \| r \| NID_{ij}')$ to pass through the authentication of U_i.

5.5 Verification table stolen attack

If an adversary can get account table $(NID_{ij}, y_i) = (NID_{ij}, E_{X_s}(ID_i, ctr_{U_i}))$, however, it is no use, since ID_i is encrypted by the medical server S_j 's secret key X_s.

5.6 Perfect forward secrecy and known key security

In the proposed scheme, the session key is $SK = h(r_2 \| r_1 \| r \| ctr'_{U_i})$, where $r_1 = aP$, $r_2 = bP$ and $r = abP$. Since a and b are random nonces chosen by U_i and S_j, respectively, which are changed in each session run. Therefore, if the adversary can know $\{X_s, ID_i, PW_i\}$, then he can know r_1, but he can not compute r from r_1 and r_2 due to the intractability of CDH problem, so our scheme provides perfect forward secrecy.

Since all the session keys are independent and dependent on random nonces a and b, so an adversary can not compute other session keys when he knows one session key.

6. Formal Verification

In this section, we use formal verification tool ProVerif [20], which is based on applied pi calculus [21] to prove the session key secrecy and authentication, instead of the formal security proof. Since the formal security proof is presented by artificial structure, and the errors may not easy to be found; while ProVerif is performed automatically, and the errors can be detected easily. On the other hand, it supports many cryptographic primitives such as symmetric and asymmetric encryption, digital signature, hash function, etc.

The ProVerif code for the definition of functions, reduction, equation, free names and constants is as follows.

```
(*function*)
fun h(bitstring):bitstring.    (*hash function*)
fun co(bitstring,bitstring):bitstring.
fun xor(bitstring,bitstring): bitstring.
fun mult(bitstring,bitstring):bitstring.
fun senc(bitstring,bitstring):bitstring. (*symmetric encryption*)
fun add(bitstring,bitstring):bitstring.
(*reduction*)
reduc forall x: bitstring, y: bitstring; sdec(senc(x, y), y) = x.
(*equation*)
equation forall x: bitstring, y: bitstring; xor(xor(x, y), y) = x.
(*free names and constants*)
const PW:bitstring [private].
const ID:bitstring [private].
const Bi:bitstring[private].
const Xs:bitstring[private].
const P:bitstring.
const k:bitstring.
const zero:bitstring.
const one:bitstring.
free SK:bitstring [private].
free SK':bitstring [private].
```

The core message sequences for the proposed scheme are given below.

Message 1: U --> S: (M1, M2, ctrU’, NID)

Message 2: S --> U: (M3, M4, r2)

Message 3: U--> S: (M5)

The protocol was modeled as the parallel execution of two processes: the patient user U and the medical server S:

```
process !U | S
```

The processes are the core of protocol model, which define the behavior of each participant in applied pi calculus. The process of user defines the behavior of U, who computes e2, r1, trU', M1 and M2, and sends message (M1, M2, ctrU’, NID) through a public channel. After that, U receives message (M3, M4, r2) and computes M5 and SKA. The process of U is modeled as below:

```
let U=
        let RPW=h(co(Bi,xor(ID,PW))) in
        let f=h(RPW) in
        out(sch,ID);
        in(sch,(NID1:bitstring,P1:bitstring,ctrU1:bitstring,e1:bitstring));
        let TID=xor(RPW,e1) in
        !
        (
          event UserStarted(ID);
          new a:bitstring;
          let e2=xor(RPW,TID) in
          let r1=mult(a,P) in
          let ctrU'=add(ctrU1,one) in
          let M1=senc(co(r1,ctrU'),e1) in
          let M2=h(co(ID,co(r1,co(ctrU',NID1)))) in
          out(sch,(M1,M2,ctrU',NID1));
          in(sch,(M3':bitstring,M4':bitstring,r2':bitstring));
          let r'=mult(a,r2')in
          let NID3=xor(h(co(r1,r')),M3') in
          let M4''=h(co(r2',co(r1,co(r',NID3)))) in
          if M4''=M4' then
          let M5=h(co(NID3,r')) in
          let SK=h(co(r2',co(r1,co(r',ctrU')))) in
          out(sch,M5);
          0
        ).
```

The process of trust sever defines the behavior of S during authentication, it authenticates the message (M1, M2, ctrU’, NID) received from U, computes and sends (M3, M4, r2) to U through a public channel. After that, S receives and verifies the message M5, and computes SK'. The process of S is modeled as follows:

```
let S=
```

```
in(sch,ID1:bitstring);
new NID:bitstring;
let e=h(co(ID,Xs)) in
let ctrU=zero in
let M=(ID,ctrU) in
let y=senc(M,Xs) in
out(sch,(NID,P,ctrU,e));
in(sch,(M1':bitstring,M2':bitstring,ctrU2:bitstring,NID2:bitstring));
let (ID2:bitstring,ctrU3:bitstring)=sdec(y,Xs) in
event UserAuthed(ID2);
let(r1':bitstring,ctrU4:bitstring)=sdec(M1',h(co(ID2,Xs))) in
let M=h(co(ID2,co(r1',co(ctrU4,NID2)))) in
if M=M2' then
new b:bitstring;
new NID':bitstring;
let r2=mult(b,P) in
let r=mult(b,r1') in
let M3=h(xor(co(r1',r),NID')) in
let M4=h(co(r2,co(r1',co(r,NID')))) in
out(sch,(M3,M4,r2));
in(sch,M5':bitstring);
let M5''=h(co(NID',r)) in
if M5'=M5'' then
let SK'=h(co(r2,co(r1',co(r,ctrU4)))) in
0.
```

The secrecy of the session key and the authentication of the protocol are modeled as:

```
query attacker(SK).
query attacker(SK').
event UserAuthed(bitstring).
event UserStarted(bitstring).
query id: bitstring; inj-event(UserAuthed(id)) ==> inj-event(UserStarted(id)).
```

We perform the above process in the latest version 1.88 of ProVerif and the performance results show that the proposed scheme achieves security and authentication.

7. Performance Comparison

In this section, we present the performance comparison among our scheme and five related schemes [15-19]. Li et al. [22,23] showed that it needs 0.0005 second for one hash operation, 0.063075 second for a scalar multiplication on elliptic curve, and 0.0087 second to perform a symmetric encryption/decryption, respectively.

Let T_m, T_h and T_s be the time for performing a scalar multiplication on elliptic curve, a one-way hash function, and a symmetric encryption/decryption, respectively. Compared to above operations, exclusive OR and string concatenation operations can be ignored. Since the registration and password change phases only perform one time or off-line, so we mainly focus on the computation of login and verification phase, which is given in Table 1.

Table 1: The computation cost comparison

	U_i	S_j	Total
Chang et al. (2013) [15]	$6T_h$	$4T_h$	$10T_h \approx 0.005s$
Das et al. (2013) [16]	$10T_h$	$7T_h$	$17T_h \approx 0.0085s$
Wen (2013) [17]	$2T_s + 9T_h$	$2T_s + 6T_h$	$4T_s + 15T_h \approx 0.0423s$
Tsai et al. (2013) [18]	$3T_m + 6T_h$	$3T_m + 4T_h$	$6T_m + 10T_h \approx 0.38s$
Tan (2014) [19]	$3T_m + 6T_h$	$3T_m + 4T_h$	$6T_m + 10T_h \approx 0.38s$
Our scheme	$2T_m + T_s + 7T_h$	$2T_m + 2T_s + 6T_h$	$4T_m + 3T_s + 13T_h \approx 0.28s$

From Table 1, we can conclude that Chang et al. [15], Das et al. [16] and Wen [17] schemes are more efficient than others, but these schemes can not achieve perfect forward secrecy. In order to achieve perfect forward secrecy, we always use the Diffie-Hellmen Key Agreement technology, but it may need more computation costs. The proposed scheme is more efficient than Tsai et al. [18] and Tan [19] schemes.

8. Conclusion

In this paper, we showed that Wen.'s scheme can not resist off-line password guessing attack, and can not provide privacy protection and perfect forward secrecy. We then propose an improved scheme to overcome their weaknesses. According to formal verification and performance analysis, we show that the proposed scheme achieves security and highly efficient for connected health care.

Acknowledgements. This research was supported by the Major State Basic Research Development (973) Program of China (No. 2013CB834205), the National Natural Science Foundation of China (No. 61070153, 61103209), and Natural Science Foundation of Zhejiang Province (No. LZ12F02005, LY12F02006).

Reference

1. Lambrinoudakis, C., and Gritzalis, S., Managing medical and insurance information through a smart-card-based information system. *J. Med. Syst.* 24(4):213–234, 2000.
2. Lee, W. B., and Lee, C. D., A cryptographic key management solution for HIPAA privacy/security regulations. *IEEE Trans. Inf. Technol. Biomed.* 12(1):34–41, 2008.
3. Wu, Z. Y., Chung, Y., Lai, F., and Chen, T. S., Password-Based User Authentication Scheme for the Integrated EPR Information System. *J. Med. Syst.* 36:631–638, 2012.
4. Wu, Z. Y., Lee, Y. C., Lai, F., Lee H. C., and Chung, Y., A Secure Authentication Scheme for Telecare Medicine Information. Systems. *J. Med. Syst.* 36:1529–1535, 2012.
5. He, D. B., Chen, J. H., and Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36:1989–1995, 2012.
6. Wei, J., Hu, X., and Liu, W., An Improved Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* 36(6): 3597-3604, 2012.
7. Zhu, Z., An Efficient Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* 36(6):3833-3838, 2012.
8. Das, M. L., Saxena, A., and Gulati, V. P., A dynamic ID-based remote user authentication scheme. *IEEE Trans. Consum. Electron.* 50(2):629–631, 2004. 508.
9. Awashti A K. Comment on a Dynamic ID-based Remote User Authentication Scheme. *Transactions on Cryptology.*, l:15–16,2014.
10. Ku W C, Chang S T. Impersonation Attack on a Dynamic ID-based Remote User Authentication Scheme using Smart Cards. *IEICE Transactions on Communications.*, *E88-B*:2165–2167,2005.
11. Wang Y Y, Kiu J Y, Xiao F X, Dan J. A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme. *Comput. Commun.* 32: 583–585,2009.

12. Khan, M. K., KS. K., and Alghathbar, K., Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme. *Comput. Commun.* 34(3):305–309, 2010.
13. Chen, H. M., Lo, J. W., and Yeh, C. K., An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. *J. Med. Syst.* 36(6): 3907-3915, 2012.
14. Xie, Q., Zhang, J., and Dong, N., Robust Anonymous Authentication Scheme for Telecare Medical Information Systems. *J. Med. Syst.* 37(2):1-8, 2013.
15. Chang, Y. F., Yu, S. H., and Shiao, D. R., An uniqueness-and anonymity-preserving remote user authentication scheme for connected health care. *J. Med. Syst.* 37:9902, 2013.
16. Das, A. K., and Goswami, A., A Secure and Efficient Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care. *J. Med. Syst.* 37:9948, 2013.
17. Wen, F., A Robust Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care. *J. Med. Syst.* 37:9980, 2013.
18. Tsai, J.,Lo, N., and Wu. T., Novel Anonymous Authentication Scheme Using Smart Cards. *IEEE Trans. Ind. Electron.*,9(4):2004-2013, 2013.
19. Tan, Z., A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* 38:16, 2014.
20. Abadi, M., Blanchet, B., and Lundh, H. C., Models and Proofs of Protocol Security: A Progress Report. *21st International Conference on Computer Aided Verification*, Grenoble, France, pp. 35-49, 2009.
21. Abadi, M., and Fournet, C., Mobile Values, New Names, and Secure Communication. *Proceedings of the 28th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*. ACM New York, pp. 104-115, 2001.
22. Li, C. T., Hwang, M. S., and Chu, Y. P., A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Comput. Commun*. 31: 2803-2814, 2008.
23. Li, W., Wen, Q., Su, Q., and Jin, Z., An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. *Comput. Commun*. 35:188-195,2012.