Liu et al. SpringerPlus (2016) 5:555
DOI 10.1186/s40064-016-2018-7

SpringerPlus

RESEARCH Open Access

An improved authenticated key agreement protocol for telecare medicine information system

Wenhao Liu, Qi Xie*, Shengbao Wang and Bin Hu

*Correspondence:
qixie68@126.com
Hangzhou Key Laboratory of Cryptography and Network Security, Hangzhou Normal University, Hangzhou 311121, China

Abstract

In telecare medicine information systems (TMIS), identity authentication of patients plays an important role and has been widely studied in the research field. Generally, it is realized by an authenticated key agreement protocol, and many such protocols were proposed in the literature. Recently, Zhang et al. pointed out that Islam et al.'s protocol suffers from the following security weaknesses: (1) Any legal but malicious patient can reveal other user's identity; (2) An attacker can launch off-line password guessing attack and the impersonation attack if the patient's identity is compromised. Zhang et al. also proposed an improved authenticated key agreement scheme with privacy protection for TMIS. However, in this paper, we point out that Zhang et al.'s scheme cannot resist off-line password guessing attack, and it fails to provide the revocation of lost/stolen smartcard. In order to overcome these weaknesses, we propose an improved protocol, the security and authentication of which can be proven using applied pi calculus based formal verification tool ProVerif.

Keywords: Authentication, Protocol, Biometrics, Smart card

Background

In Internet environment, especially in the C/S model, it is crucial to authenticate both the user and the server when the user needs to access services provided by the server (Khan et al. 2014). The telecare medicine information system (TMIS) has attracted great attention of researchers to establish a convenient communication over the Internet between patients at home and doctors at a clinical center or home health-care agency (Kaul and Awasthi 2013; Wen 2013). A doctor can easily get access to his patient's medical history from TMIS, and diagnose quickly without repeating physical examination. Besides, TMIS can save the patients' expenses and time (Xie et al. 2014). However, it is a great challenge to preserve the security and privacy of patient's information transmitted over the Internet (Xie et al. 2013; Siddiqui et al. 2014).

Related works

Wu et al. (2010) proposed the first two-factor authentication scheme for TMIS service. Since then, a lot of two-factor authentication protocols have been proposed (He et al. 2012; Wei et al. 2012; Zhu 2012; Muhaya 2015). He et al. (2012) showed that Wu et al.'s

protocol could not resist insider attack and impersonation attack. And they gave an improved protocol using smartcard. However, Wei et al. (2012) showed that He et al.'s protocol failed to resist off-line password guessing attack, and they also proposed an improved scheme, but Wei et al.'s scheme has the same security defects. In order to fix the above drawbacks, Zhu (2012) proposed an improved scheme. Unfortunately, Zhu et al.'s scheme has been proven insecure by Muhaya (2015). Wu et al. (2012) proposed a password-based user authentication scheme for the integrated EPR information system. Later, Islam and Biswas (2014) found that Wu et al.'s (2012) scheme cannot resist privileged-insider attack, off-line password guessing attack and ephemeral secret leakage attack.

It's an interesting topic to improve security and computation efficiency of the authentication schemes. Pu et al. (2010) designed an anonymous authentication scheme for TMIS service using the elliptic curve cryptography (ECC). Chen et al. (2012) proposed a dynamic-identity based authentication scheme for TMIS. However, Jiang et al. (2013) showed Chen et al.'s scheme (Chen et al. 2012) cannot withstand impersonation attack, off-line password guessing attack and denial-of-service attack. Recently, Xu et al. (2014) proposed a two-factor authentication key agreement protocol using ECC. Unfortunately, Islam and Khan (2014) showed that Xu et al.'s scheme (Xu et al. 2014) can neither withstand replay attack, nor provide the revocation of lost/lost smart or achieve strong authentication in login and authentication phases. In order to overcome the above defects, they proposed a new anonymous two-factor authentication protocol for TMIS. Recently, Zhang and Zhou (2015) pointed out that Islam et al.'s protocol has many security defects such as: (1) Any legal but malicious patient can reveal other user's identity; (2) An attacker can launch off-line password guessing attack and the impersonation attack if he knows legal user's identity. Zhang et al. then proposed a new ECC-based authenticated key agreement scheme in order to fix the above security problems. In 2015, Chaudhry et al. (2015) also showed that Islam et al.'s protocol (Islam and Khan 2014) suffers from user impersonation attacks and server impersonation attacks. And then they proposed an improved two-factor authentication protocol for TMIS. In fact, Chaudhry et al.'s scheme is insecure under lost/stolen smartcard disguised attack and off-line password guessing attack, for that an insider adversary can extract information $(r_i, h())$ from the memory of the user's smart card. As we generally use passwords which are low-entropy keys, the following attack is feasible in practice: suppose that PW' is the guessed password and l_i is the user's identity, an insider adversary (e.g. a malicious server) can compute $l_i' = h(ID_i||PW'||r_i)$; if $l_i' = l_i$, then the adversary successfully found the correct password PW_i.

As biometric keys can maintain uniqueness property, they can neither be forged nor guessed easily. Therefore, biometric keys have been widely adpoted in authentication protocols. In 2010, Li and Hwang (2010) proposed a biometric based remote user authentication scheme using user's biometric key to identify the correct user. Li et al. (2011) showed that Li and Hwang's scheme is vulnerable to man-in-the-middle attack, and they proposed an improved biometrics-based remote user authentication scheme. However, Truong et al. (2012) pointed that Li et al.'s scheme cannot resist stolen verifier attack, reply attack and man-in-the-middle attack, and they proposed an improved remote user authentication scheme. However, the login and password change phase of

their scheme is not efficient for practice. Later, Awasthi and Srivastava (2013) proposed a new robust biometrics-based remote user authentication scheme using smart cards in order to avoid the time-consuming exponential operations. Unfortunately, Dheerendra et al. (2014) demonstrated that Awasthi et al.'s scheme fails to resist online and off-line password guessing attack, and they proposed an improved biometrics-based authentication scheme for TMIS. In 2014, He and Wang (2014) proposed a robust multi-server authentication scheme using biometrics-based smart card. But Vanga et al. (2015) pointed that He and Wang's scheme is vulnerable to a known session-specific temporary information attack and impersonation attack. And they proposed a secure biometrics-based multi-server authentication protocol using biometrics-based smart card, and provided simulation results of their scheme for the formal security verification using Automated Validation of Internet Security Protocols and Applications (AVISPA) tool (AVISPA; Lv et al. 2013).

Our contributions

In this paper, we show that Zhang et al.'s protocol (Zhang and Zhou 2015) is vulnerable to lost/stolen smartcard disguised attack and off-line password guessing attack. And then we propose an improved protocol using biometric keys (fingerprint, face and palmprint, etc.) to resolve the security problems. Furthermore, we provide the simulation results of our scheme for the formal security verification, using applied pi calculus based formal verification tool ProVerif. Our protocol overcomes the weaknesses of Islam et al.'s scheme and Zhang et al.'s scheme, and has the similar efficiency in comparison with their schemes.

The rest of paper is organized as follows: we first review Zhang et al.'s protocol in second section, and show the security weaknesses of Zhang et al.'s protocol in third section. Then, we propose an improved authentication protocol for TMIS is in fourth section. The security analysis of the improved scheme is given in fifth section. We prove the session key secrecy and authentication property using pi calculus based ProVerif in sixth section. In seventh section, we compare security and computation cost between our scheme and other related schemes. We conclude the paper in eighth section.

Review of Zhang et al.'s scheme

In this section, we review Zhang et al.'s scheme. There are two participants in Zhang et al.'s protocol, patient U and telecare server S. Table 1 shows the notations used in this paper.

Initialization phase

S selects an elliptic curve $E_p(a, b)$ over a prime finite field F_p and a base point P over $E_p(a, b)$. Followed that, S chooses a random number $s \in Z_p^*$ as his secret value, and computes $Q_s = sP$, and selects a one-way hash function $H(\cdot) : \{0,1\}^* \rightarrow Z_p^*$, and publishes $\{E_p(a, b), P, H(\cdot), Q_s\}$ and keeps s as a secret value.

Registration phase

1. U selects his identity ID, its password PW and a random number r, and computes $l = H(r||PW)$ and sends (ID, l) to S via a secure way.

Table 1 The notations

Notations	Description
U	Patient in TMIS
S	Telecare server in TMIS
ID	Patient U's identity
PW	Patient U's password
s	Telecare server's secret key
Q_s	Telecare server's public key, where $Q_s = sP$
E_k/D_k	Symmetric encryption/decryption algorithm with key k
$H(\cdot)$	Secure one-way collision-resistant hash function
$\|\|$	String concatenation operation
$\oplus$	Exclusive OR operation

2. Upon receiving (ID, l), S verifies user's legitimacy in his database. If ID is a new patient, S sets $N = 0$, otherwise, U is re-registering to the system, S sets $N = N + 1$, and stores (ID, N, T) into its database, where T is the current registration time.
3. S computes $\sigma = H(s \oplus ID)$, $v = \sigma \oplus l$, $\mu = H(ID \oplus l)$ and stores $\{v, \mu, P, H(\cdot), N, E_p(a, b)\}$ into the smart card, and sends it to U via a secure way.
4. On obtaining the smartcard, U stores the number r in it.

Login and authentication phase

1. U inserts his smart card into the terminal and inputs his identity ID and password PW. The smartcard computes $l = H(r||PW)$, $\mu' = H(ID \oplus l)$, and checks whether $\mu' = \mu$ holds. If not, it aborts the session; otherwise, it selects a random number a and a current timestamp T_1. Then, smartcard computes $V = aP$, $I = aQ_s$, $K_u = H(I||T_1)$, $\sigma = v \oplus l$, $D = H(V||N||\sigma)$ and $G_1 = E_{K_U}(ID||D)$. Then, smartcard sends login information $m_1 = \{V, G_1, T_1\}$ to U via the public channel.
2. After receiving m_1 at T_2, S checks whether $T_2 - T_1 < \Delta T$ is valid. If it is true, S computes $I = sV$, $K_s = H(I||T_1)$, and decrypts G_1 to get ID' and D', and checks if ID' is found in the database. If not, S terminates the session; otherwise, S computes $\sigma^* = H(s \oplus ID')$ and checks whether $D' = H(V||N||\sigma^*)$ holds. If not, this session terminates; otherwise, S selects a random number c and computes $W = cP$, $J = cV$, $sk_s = H(ID'||I||J)$, $G_2 = H(\sigma^*||ID'||sk_s||W||T_2)$, and S sends $m_2 = \{W, G_2, T_2\}$ to U via the public channel. If T_2 is invalid, abort, otherwise, smartcard computes $J = aW$, $sk_u = H(ID||I||J)$, $G_2' = H(\sigma||ID||sk_u||W||T_2)$, and checks whether $G_2' = G_2$ holds. If not, it aborts the session; otherwise, U authenticates S successfully.

Password updating phase

U inserts his smart card into the terminal and enter his ID and PW when he wants to update its password.

1. The smartcard computes $l = H(r||PW)$, $\mu' = H(ID \oplus l)$, and checks whether $\mu' = \mu$ holds. If not, it aborts the session; otherwise, it selects a new random number r^* and a new password PW^*, and updates corresponding value in the smart card.

2. The smartcard computes $\sigma = v \oplus l, l^* = H(r^*||PW^*), v^* = \sigma \oplus l^*, \mu^* = H(ID \oplus l^*)$ and replaces (v, μ) with (v^*, μ^*), respectively.

Lost/stolen smartcard revocation phase

When U's smartcard is lost or stolen, it will request S for its revocation.

1. U chooses its new password PW^* and new random number r^*, and computes $l^* = H(r^*||PW^*)$, and submits (ID, l^*) to S over a secure channel.
2. S firstly checks the registration credentials of U. If the credential provided by U is valid, S updates N as $N = N + 1$ for the tuple (ID, N, T_1) to revoke the smartcard.
3. S computes $\sigma = H(s \oplus ID)$, $v^* = \sigma \oplus l^*$, $\mu^* = H(ID \oplus l^*)$, and stores $\{v^*, \mu^*, P, H(\cdot), Q_s, N, E_p(a, b)\}$ into the smart card, and sends it to U via a secure way.
4. On obtaining the smartcard, U stores the random number r^* in it. Finally, the smartcard stores $\{r^*, v^*, \mu^*, P, H(\cdot), Q_s, N, E_p(a, b)\}$.

Weaknesses of Zhang et al.'s scheme

Through careful analysis, we find that Zhang et al.'s protocol is vulnerable to off-line password guessing attack and lost/stolen smartcard disguised attack. The detailed analyses are described as follows.

Off-line password guessing attack

If an insider adversary in TMIS can extract information (r, μ) from the memory of the user's smart card (Zhang and Zhou 2015). Generally speaking, password is not high-entropy keys (Abadi and Fournet 2001). Therefore, the following attack is feasible in practice. Suppose that PW' is the guessed password, and an insider adversary (e.g. the user's colleague or malicious server) may know the user's identity easily.

The insider adversary in TMIS who knows ID can compute $l' = H(r||PW')$, $\mu' = H(ID \oplus l') = H(ID \oplus H(r||PW'))$, and checks whether $\mu' = \mu$ holds. If it is true, the insider adversary has guessed the correct password. Otherwise, it repeatedly guesses a new password until he succeeds.

Failure to provide the revocation of lost/stolen smartcard

Though the Zhang et al.'s scheme has lost/stolen smartcard revocation phase, an insider adversary can still use the lost/stolen smartcard to pass through the authentication process. The reason is that $\sigma = H(s \oplus ID)$ and ID in the new smart card are the same as that of the lost/stolen smartcard, and $N = N + 1$, according to off-line password guessing attack, the adversary can easily get PW and compute the correct authentication request message $m_1 = \{V, G, T_1\}$, which can pass the authentication of the server.

The improved scheme

In our improved scheme, $\{s, E_p(a, b), P, H(\cdot), Q_s\}$ are the same as that of Zhang et al.'s scheme.

Registration phases

When a user U wants to become a legal user, he should register to S as follows.

1. U selects his identity ID, password PW and a random number r, and computes $l = H(r||PW)$, and sends (ID, l) to S via a secure way.
2. Upon receiving (ID, l), S verifies user's legitimacy in his database. If ID is a new patient, S sets $N = 0$, otherwise, U is re-registering to the system, S sets $N = N + 1$, and stores the tuple (ID, N, N_c) to its database, where N_c is the identity of the smart card.
3. S computes $\alpha = H(s \oplus ID)$, $\beta = \alpha \oplus l$ and stores $\{\beta, P, H(\cdot), Q_s, N, N_c, E_p(a, b)\}$ into the smart card, and sends it to U via a secure way.
4. On obtaining the smartcard, U scans and enters his personal biometrics Bio. It is worth mentioning that no one can get Bio except U and the biometrics scanner can be combined in the smart card reader. U computes $\mu = r \oplus H(Bio)$, $\theta = H(ID||PW||r)$, U stores (μ, θ) in the smart card.

Login and authentication phases

In this phase, the user U and the server S can be authenticated each other and establish the session key sk, which showed in Algorithm 1.

1. U inserts his smart card into the terminal and inputs his identity ID, password PW and Bio. The smartcard computes $r' = \mu \oplus H(Bio)$, $\theta' = H(r'||PW||ID)$, and checks whether $\theta' = \theta$ holds. If not, it aborts the session; otherwise, it selects two random numbers a and N_1. Then, smartcard computes $V = aP$, $I = aQ_s$, $K_u = H(I||N_1)$, $\alpha = \beta \oplus l$, $\gamma = H(V, N, N_1, \alpha, N_c)$ and $G_1 = E_{K_U}(ID||N_1||\gamma||N_c)$. Then, smartcard sends login information $m_1 = \{V, G_1, N_1\}$ to S via the public channel.
2. After receiving m_1, S checks whether N_1 is a fresh nonce or not. If it is true, S computes $I = sV$, $K_s = H(I||N_1)$, and decrypts G_1 to get ID', N_c, γ and N_1, and checks whether or not ID' is found in the database. If not, S terminates the session; otherwise, S computes $\alpha^* = H(s \oplus ID)$, $\gamma^* = H(V, N, N_1, \alpha^*, N_c)$, and checks whether $\gamma^* = \gamma$ holds. If is not true, S terminates the session; otherwise, it selects two random numbers c and N_2 for computing $W = cP$, $J = cV$, $K = H(J||N_2)$ $G_2 = E_K(Q_s||N_2)$, $sk = H(ID'||Q_s||I||J||N_1||N_2)$, and S sends $m_2 = \{W, G_2, N_2\}$ to U via the public channel. If N_2 is not a fresh nonce number, abort, otherwise, smartcard computes $J = aW$, $K = H(J||N_2)$, and decrypts G_2 to get Q_s and N_2, and checks whether or not $Q_s' = Q_s$ holds. If not, smartcard terminates the session; otherwise, U authenticates S successfully, and computes $sk = H(ID||Q_s||I||J||N_1||N_2)$.

U	S
Input ID, PW and Bio	
$r^{'} = \mu \oplus H(Bio)$, $\theta^{'} = H(ID \| PW \| r^{'})$	
if $(\theta^{'} \neq \theta)$, abort	
else, $a \in_R Z_p^*, N_1$	
$V = aP, I = aQ_S$	
$K_u = H(I \| N_1), \alpha = \beta \oplus l$	
$\gamma = H(V, N, N_1, \alpha, N_c)$	
$G_1 = E_{K_U}(ID \| N_1 \| \gamma \| N_c)$, $\xrightarrow{m_1=\{V, G_1, N_1\}}$	if N_1 isn't fresh, abort
	else, $I = sV, k_s = H(I \| N_1)$
	$ID^{'} \| N_1 \| \gamma \| N_c = D_{k_s}(G_1)$
	$\alpha^* = H(s \oplus ID)$
	if $\gamma^* \neq H(V, N, N_1, \alpha^*, N_c)$, abort
	else, $c \in_R Z_p^*$
	$W = cP$, $J = cV$
	$K = H(J \| N_2)$
if N_2 isn't fresh, abort $\xleftarrow{m_2=\{W, G_2, N_2\}}$	$G_2 = E_K(Q_s \| N_2)$
else, $J = aW$, $K = H(J \| N_2)$	
$Q_s^{'} \| N_2 = D_K(G_2)$	
If $Q_s^{'} \neq Q_s$, abort	
else, accept the session key $sk = H(ID \| Q_s \| I \| J \| N_1 \| N_2)$	

Algorithm 1 Login and authentication phases

Password updating phases

U inserts his smart card into the terminal and enter his *ID* and *PW* when he wants to update its password.

1. The smartcard computes $r' = \mu \oplus H(Bio)$, $l = H(PW||r')$, $\theta = H(ID||PW||r')$ and checks whether $\theta' = \theta$ holds. If not, it aborts the session; otherwise, it selects a new

random number r^* and a new password PW^*, and updates corresponding value in the smart card.
2. The smartcard computes $\mu^* = r^* \oplus H(Bio)$, $\theta^* = H(ID||PW^*||r^*)$ and replaces (μ, θ) with (μ^*, θ^*).

Lost/stolen smartcard revocation phases

When U's smartcard is lost or stolen, it will request S for its revocation.

1. U chooses its new password PW^* and new random number r^*, and computes $l^* = H(r^*||PW^*)$, $\mu^* = r^* \oplus H(Bio)$, $\theta^* = H(ID||PW^*||r^*)$ and submits $(ID, l^*, \mu^*, \theta^*)$ to S over a secure channel.
2. S checks the registration credentials of U. If the credential provided by U is valid, S updates N as $N = N + 1$ for the tuple (ID, N, N_c) to revoke the smartcard, and deletes N_c from his database and selects a new smartcard number N_{new} for U, and returns the tuple (ID, N, N_{new}) to his database.
3. S computes $\alpha = H(s \oplus ID)$, $\beta^* = \alpha \oplus l^*$, $\theta^* = H(ID||PW||r^*)$, and stores $\{\beta^*, P, H(\cdot), Q_s, N, N_{new}, E_p(a, b)\}$ into the smart card, and sends it to U via a secure way.
4. On obtaining the smartcard, U stores (μ^*, θ^*) in it. Finally, the smartcard stores $\{\theta^*, \mu^*, \beta^*, P, H(\cdot), Q_s, N, N_{new}, E_p(a, b)\}$.

Security analysis

In this section, we analyze the security of the improved protocol. The following attacks assume that a malicious adversary can eavesdrop, modify, insert, or delete any messages transmitted via public channel.

The improved protocol can achieve mutual authentication

As $V = aP$, $I = aQ_s$, $K_u = H(I||N_1)$, and $G_1 = E_{K_U}(ID||N_1||\gamma||N_c)$, only the legal user U can get the secret value (I, N_1) to generate a legal G_1. S decrypts G_1 and checks whether $ID' = ID$ holds. If it is true, S can authenticate U, otherwise, U cannot be authenticated by S. On the other hand, U can authenticate S by verifying whether $Q_s' = Q_s$ hold. As a result, our protocol achieves the mutual authentication.

Malicious insider impersonation attack

Login phase: If a malicious user U_A wants to impersonate U, he must forge a valid login message $\{V^*, G_1^*, N_1\}$ where $V^* = a^*P$, $I^* = a^*Q_s$, $K^* = H(I^*||N_1)$, and $G_1^* = E_{K^*}(ID^*||N_1||\gamma||N_c)$, however, U_A can not get I, such that it has to forge an invalid one. When S receives the login request message from U, it will decrypt and compute $G_1^* = E_{K^*}(ID^*||N_1||\gamma||N_c)$, but the equation $ID^* = ID$ does not hold, therefore, S will reject the login request. Thus, our scheme can resist insider impersonation attack.

Off-line password guessing attack

If a malicious attacker has stolen user's smart card, then he can extract the information $\{\theta, \mu, \beta, P, H(\cdot), N, Q_s, E_p(a, b)\}$ from the smart card, where $\mu = r \oplus H(Bio)$, $\theta = H(ID||PW||r)$, $l = H(r||PW)$. Since r is protected by Bio and PW is protected by

a one-way hash function, the attacker cannot know both of the real identity ID and the correct password PW. It is impossible to guess these two parameters correctly in polynomial time. Therefore, our protocol is secure against the off-line password guessing attack.

Strong replay attack

If a malicious attacker wants to replay a previously transmitted message of the sender or the receiver, the attack will fail since U and S choose different random numbers (N_1, N_2) in each session. During the authentication phase, after S response the next login message $m_1' = \{V', G_1', N_1'\}$ using a valid nonce N_1, the attacker can neither verify its validness nor obtain the session key assuming the intractability of Diffie–Hellman problem.

Lost/stolen smartcard attack

When the attacker attempts to insert the lost smart card into the device, it can't pass the authentication of the server, since the stolen card's N_c is updated in the database of S.

Perfect forward secrecy

In our protocol, the session key is $sk = H(ID||Q_s||I||J||N_1||N_2)$, where $I = aQ_s = asP$, $J = cV = caP$. Since a and c are random numbers chosen by U and S, their values are changed in each session run. Therefore, our protocol can provide perfect forward secrecy.

Formal verification

Some formal verification tools are used to prove the security of cryptographic protocols, such as BAN logic, AVISPA and ProVerif (Abadi et al. 2009). In this section, we prove the session key secrecy and authentication using formal verification tool ProVerif, which is based on applied pi calculus (Abadi and Fournet 2001). The reason is that ProVerif is performed automatically, and the errors can be detected easily, while the formal security proof is artificial structured, and the errors may not easy to be found.

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

```
(* ----------channel----------*)
sch: secure channel between S and U.
free sch: channel [private].

(*----------variables and constants----------*)
const ID: bitstring.
const PW: bitstring [private].
const Nc: bitstring [private].
const P: bitstring.
const zero: bitstring.
const one: bitstring.
free s: bitstring [private].
free sk:bitstring [private].
free sku:bitstring [private].

(*----------constructor----------*)
fun H(bitstring): bitstring.
fun senc(bitstring, bitstring): bitstring.
fun or(bitstring, bitstring): bitstring.
fun exp(bitstring, bitstring): bitstring.
fun xor(bitstring, bitstring): bitstring.
fun add(bitstring, bitstring): bitstring.
fun mult(bitstring, bitstring): bitstring.
(*----------destructors & equations----------*)
reduc forall m: bitstring, n: bitstring; sdec(senc(m, n), n) = m.
equation forall m: bitstring, n: bitstring; xor(xor(m, n), n) = m.
(*----------events----------*)
event UserAuthed(bitstring).
event UserStarted(bitstring).
(*----------query----------*)
```

```
query attacker(sku).
query attacker(sk).
query id: bitstring; inj-event(UserAuthed(id)) ==> inj-event(UserStarted(id)).
(*------------------processes-------------------------*)
let U=
        new r: bitstring;
      let l=H(or(r,PW)) in
      out(sch,(ID,l));
in (sch,(d':bitstring,P':bitstring,Qs': bitstring,N":bitstring,Nc':bitstring));
      new Bio: bitstring;
      let u=xor(r,H(Bio)) in
        !
        (
        event UserStarted(ID);
        let r'=xor(u,H(Bio)) in
      let u'=H(or(r',or(PW,ID))) in
      if u=u' then
      new a: bitstring;
      new N1: bitstring;
      let V=mult(a,P) in
      let I=mult(a,Qs') in
      let Ku=H(or(I,N1)) in
      let f'=xor(d',l) in
      let m1=(V,N",N1,f',Nc) in
      let r"=H(m1) in
      let G1=senc(or(ID,or(N1, or(r",Nc))),Ku) in
      out(sch,(V,G1,N1));
      in(sch,(W': bitstring,G2": bitstring,N2': bitstring));
      let J'=mult(a,W') in
      let K'=H(or(J',N2')) in
```

```
        let (Qs'': bitstring,N2'': bitstring)=sdec(G2'',K') in
        if Qs'=Qs'' then
        let sku= H(or(ID,or(Qs'',or(I,or(J',or(N1,N2'')))))) in
          0
          ).
let S =
   in(sch, (ID': bitstring,l': bitstring));
new N: bitstring;
let N'= if ID' =ID then zero else add(N,one) in
let f=H(xor(s,ID')) in
let d=xor(f,l') in
let Qs=mult(s,P) in
        out(sch,(d,P,Qs,N',Nc));
        in(sch,(V': bitstring,G1': bitstring,N1': bitstring));
        let I'=mult(s,V') in
        let Ks=H(or(I', N1')) in
        let (ID'': bitstring,N1': bitstring,r1: bitstring, Nc: bitstring)=sdec(G1',Ks) in
        event UserAuthed(ID'');
        if ID'=ID'' then
        let f2=H(xor(s,ID'')) in
        let m2=(V',N',N1', f2) in
        let r2=H(m2) in
        if r1=r2 then
        new c: bitstring;
        new N2: bitstring;
        let W=mult(c,P) in
        let J=mult(c,V') in
        let K=H(or(J,N2)) in
        let G2=senc(or(Qs,N2),K) in
        let sk=H(or(ID'',or(Qs,or(I',or(J,or(N1',N2)))))) in
        out(sch,(W,G1',N2)).
        process !U | S
```

We perform the above process in the latest version 1.88 of ProVerif. The performance results as shown in the Fig. 1. The experimental results show that our scheme is security.

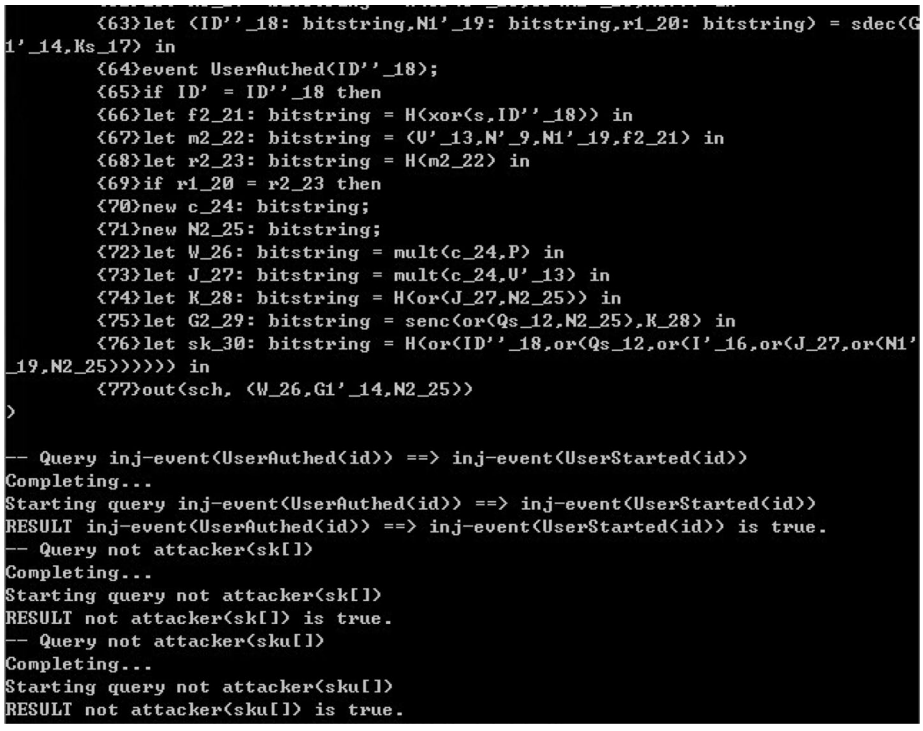

Fig. 1 The performance result

Security and computation cost comparisons

The security comparison between our scheme and other recently proposed related schemes are given in Table 2.

Let T_m be the time complexity of point multiplication in a group, T_a be the time complexity of point addition in a group, T_s be a symmetric key encryption/decryption operation and T_h be a one-way hash operation. Table 3 illustrates the average running times of some commonly used operations estimated by Kilinc and Yanik (2014), and shows that point multiplication in a group is slower than point addition, hash function and symmetric encryption/decryption operation.

Since Islam et al.'s scheme (Islam and Khan 2014) and Zhang et al.'s scheme (Zhang and Zhou 2015) are more efficient than other schemes. Therefore, in this section, we only present the computation comparison between our scheme and Islam et al.'s and Zhang et al.'s schemes, and very recently proposed related schemes, which showed in Table 4. From Table 4, we can see that our protocol is almost efficient than that of Zhang et al.'s and Islam et al.'s schemes. However, our protocol overcomes the weaknesses of Islam et al.'s and Zhang et al.'s schemes.

If the scheme can prevent the attack or satisfy the property, the symbol 'Y' is used. Otherwise, the symbol 'N' is used.

Conclusion

In this paper, we have shown that Zhang et al.'s protocol cannot achieve some secure properties, including security against off-line password guessing attacks, and it fails to provide the revocation of lost/stolen smartcard. Technically, we adopt random numbers

Table 2 Security comparison between our scheme and other schemes

Security attributes/schemes	Li and Hwang (2010)	Li et al. (2011)	Truong et al. (2012)	Awasthi and Srivastava (2013)	Dheerendra et al. (2014)	He and Wang (2014)	Vanga et al. (2015)	Ours
Provide user anonymity	N	N	Y	Y	N	N	Y	Y
Insider attack	N	Y	Y	Y	N	Y	Y	Y
Stolen smart card attack	Y	Y	Y	Y	N	Y	Y	Y
Replay attack	Y	Y	Y	Y	Y	N	Y	Y
Off-line password guessing attack	Y	Y	Y	N	Y	Y	Y	Y
Mutual authentication	N	Y	Y	N	Y	Y	Y	Y
Known session-specific temporary information attack	N	N	N	N	N	N	Y	Y
Perfect forward secrecy	N	N	N	N	N	Y	Y	Y
Impersonation attack	N	N	N	N	N	N	Y	Y
Provide lost smart-card revocation	N	N	N	N	N	N	Y	Y
Server spoofing attack	N	N	N	N	N	Y	Y	Y
Efficient login phase	N	N	N	Y	Y	Y	Y	Y
Efficient password change phase	N	N	N	N	Y	Y	Y	Y
Biometric update phase	N	N	N	N	N	Y	Y	Y

Table 3 The running time of different operations

Operations	Point multiplication	Point addition	Hash function	Symmetric encryption/decryption
Time (ms)	2.226	0.0288	0.0023	0.0046

Table 4 Computation cost comparison in login and authentication phase

	Islam and Khan (2014)	Zhang and Zhou (2015)	Chaudhry et al. (2015)	Vanga et al. (2015)	Ours
Computational cost	$6T_m + 1T_a + 10T_h$	$6T_m + 2T_s + 11T_h$	$7T_m + 8T_h$	$5T_m + 3T_s + 13T_h$	$6T_m + 4T_s + 11T_h$
Estimated time (ms)	13.4078	13.3905	15.6004	13.4767	13.3997

based authentication mechanism, instead of the timestamps that may cause time synchronization problem. An improved protocol is proposed in order to overcome those weaknesses. The simulation results show that when compared with existing protocols, our protocol provides the same level of efficiency and better security guarantees for TMIS applications.

Authors' contributions

Conceived and designed the experiments: QX. Performed the experiments: BH. Analyzed the data: SBW. Contributed reagents/materials/analysis tools: WHL, QX. Wrote the paper: WHL, QX, SBW. Designed the scheme and wrote the paper: WHL, QX, SBW. Proved the authentication and security of the proposed scheme: BH. Verified the authentication and security of the proposed scheme in the latest version 1.88 of ProVerif: BH. All authors read and approved the final manuscript.

Authors' information

Wenhao Liu received the Ph.D. degree from University of Electronic Science and Technology of China in 2010. Currently, he is a lecturer in the school of Information Science and Engineering, Hangzhou Normal University, China. His research area is applied cryptography, including digital signatures, cloud computing security and key agreement protocols etc. Qi Xie is a professor in Key Laboratory of Cryptography and Network Security, Hangzhou Normal University, China. He received his Ph.D. degree in applied mathematics from Zhejiang University, China, in 2005. He was a visiting scholar between 2009 and 2010 at Department of Computer Science, University of Birmingham in UK, and a visiting scholar to the Department of Computer Science at City University of Hong Kong in 2012. His research area is applied cryptography, including digital signatures, authentication and key agreement protocols etc. He has published over 60 research papers in international journals and conferences, and served as co-chair of ISPEC 2012 and ASIACCS 2013. Shengbao Wang received his PhD degree in computer science from Shanghai Jiao Tong University in 2008 and is now working as an associate professor at the Department of Computer Science and Engineering, Hangzhou Normal University, China. His research interests lie in the area of public key cryptography, especially focus on public key encryption and key agreement protocols. Bin Hu received the Ph.D. degree from Zhejiang University in 2009, China. Currently, he is a lecturer in the school of Information Science and Engineering, Hangzhou Normal University, China. His research mainly concerns reasoning about communication protocols, especially verification of their properties. In particular, he works on logic and calculus based specification and verification of protocols.

Acknowledgements

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

Competing interests

The authors declare that they have no competing interests.

Received: 11 August 2015 Accepted: 16 March 2016
Published online: 03 May 2016

References

Abadi M, Fournet C (2001) Mobile values, new names, and secure communication. In: Proceedings of the 28th ACM SIGPLAN-SIGACT symposium on principles of programming languages. ACM New York, 2001, pp. 104–115

Abadi M, Blanchet B, and Lundh HC (2009) Models and proofs of protocol security: a progress report. In: 21st international conference on computer aided verification, Grenoble, France, 2009, pp 35–49

Automated Validation of Internet Security Protocols and Applications (AVISPA). http://www.avispa-project.org/. Accessed 6 Jan 2015

Awasthi AK, Srivastava K (2013) A biometric authentication scheme for telecare medicine information systems with nonce. J Med Syst 37(5):1–4

Chaudhry S, Naqvi H, Shon T (2015) Cryptanalysis and improved two factor authentication protocol for telecare medicine information systems. J Med Syst 39:66
Chen H, Luo J, Yeh C (2012) An efficient and secure dynamic id-based authentication scheme for telecare medical information system. J Med Syst 36(6):3907–3915
Dheerendra M, Sourav M, Saru K (2014) Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. J Med Syst 38:41
He DB, Wang D (2014) Robust biometrics-based authentication scheme for multi-server environment. IEEE Syst J. doi:10.1109/JSYST.2014.2301517
He DB, Chen JH, Zhang R (2012) A more secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1989–1995
Islam SH, Biswas GP (2014) Cryptanalysis and improvement of a password-based user authentication scheme for integrated EPR information system. J King Saud Univ Comput Inf Sci 25:51–61
Islam S, Khan M (2014) Cryptanalysis and improved of authentication and key agreement protocols for telecare medicine information systems. J Med Syst 38:135
Jiang Q, Ma J, Ma Z (2013) A privacy enhanced authentication and key agreement scheme for telecare medicine information systems. J Med Syst 37:8979
Kaul SD, Awasthi AK (2013) RFID authentication protocol to enhance patient medication safety. J Med Syst 37:9979
Khan SU, Lavagno L, Pastrone C (2014) Online authentication and key establishment scheme for heterogeneous sensor networks. Int J Distrib Sens Netw 2014. Article ID 718286
Kilinc HH, Yanik T (2014) A survey of SIP authentication and key agreement schemes. IEEE Commun Surv Tutor 16(2):1005–1023
Li CT, Hwang MS (2010) An efficient biometrics-based remote user authentication scheme using smart cards. J Netw Comput Appl 33(1):1–5
Li X, Niu JW, Ma J (2011) Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. J Netw Comput Appl 34(1):73–79
Lv C, Ma M, Li H (2013) An novel three-party authenticated key exchange protocol using one-time key. J Netw Comput 36(1):498–505
Muhaya FT (2015) Cryptanalysis and security enhancement of Zhu's authentication scheme for telecare medical information systems. Secur Commun Netw 8(2):149–158
Pu Q, Wang J, Zhao R (2010) Strong authentication scheme for telecare medicine information systems. J Med Syst 36(4):2609–2619
Siddiqui Z, Abdullah AH, Khan MK, Alghamdi AS (2014) Smart environment as a service: three factor cloud based user authentication for telecare medical information system. J Med Syst 38:9997
Truong TT, Tran MT, Duong AD (2012) Robust biometrics based remote user authentication scheme using smart cards. In: 15th IEEE international conference on network-based information systems (NBiS'2012), pp 384–391
Vanga O, Ashok K, Adrijit G (2015) A secure biometrics-based multi-server environment authentication protocol using smart cards. IEEE Trans Inf Forensics Secur 10(9):1953–1966
Wei J, Hu X, Liu W (2012) An improved authentication scheme for telecare medicine information systems. J Med Syst 36(6):3597–3604
Wen F (2013) A robust uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. J MedSyst 37:9980
Wu ZY, Lee YC, Lai F, Lee HC, Chung Y (2010) A secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1529–1535
Wu ZY, Chung Y, Lai F, Chen TS (2012) A password-based user authentication scheme for the integrated EPR information system. J Med Syst 36(2):631–638
Xie Q, Zhang J, Dong N (2013) Robust anonymous authentication scheme for telecare medical information systems. J Med Syst 37(2):1–8
Xie Q, Liu WH, Wang SB (2014) Improvement of a uniqueness-and-anonymity-preserving user authentication scheme for connected health care. J Med Syst 38(9):91
Xu X, Zhu P, Wen Q (2014) A secure and efficient authentication scheme for telecare medicine information systems. J Med Syst 38:9994
Zhang L, Zhou S (2015) Roubust ECC-based authenticated key agreement scheme with privacy protection for telecare medicine information systems. J Med Syst 39:49
Zhu ZA (2012) An efficient authentication scheme for telecare medical information platform. J Med Syst 36(6):3833–3838