An Improved User Authentication and Key Agreement Scheme for Multi-medical Server Usable in TMIS

Hao Lin¹,ᵃ, Fengtong Wen¹,ᵇ,ᵃ, Chunxia Du¹,ᶜ

¹School of Mathematical Science, University of Jinan, 250022 Jinan, China
ᵃlinhao_ujn@163.com,ᵇwftwq@163.com,ᶜ15098823621@163.com

*Corresponding author

Keywords: TMIS, Medical services, Mutual authentication, Security, Biometric.

Abstract. Recently, Amin and Biswas proposed a novel authentication protocol for TMIS. They claimed that their protocol provides security protection on the attacks proposed by them. Even though Amin and Biswas’s protocol achieves efficiency, we demonstrate that their protocol is insecure against many attacks. To overcome the defects in Amin and Biswas’s protocol, we proposed an improved user authentication scheme in TMIS. The security analysis shows that the proposed protocol remedies the weaknesses in Amin and Biswas’s protocol.

Introduction

As a viable solution to the continuously rising demand in medical and healthcare services, TMIS employs information and communication technologies to provide remote services that assists with certain healthcare activities. TMIS establishes a secure communication platform between the patients at home and doctors through public networks.

Because of the important properties of biometrics [1], it is desirable to combine smart card with biometric to design more secure authentication schemes for TMIS [2]. In 2015, Amin and Biswas proposed a novel authentication scheme for multi-medical server in TMIS [3]. Unfortunately, we demonstrate that Amin and Biswas’s protocol will be compromised under user impersonation attacks, off-line password guessing attacks, replay attacks, privilege insider attacks, and fails to achieve forward secrecy. To eliminate the shortcomings in Amin et al.’s protocol [3], we proposed an improved user authentication scheme for TMIS, which withstands many well-known traditional attacks.

Review of Amin and Biswas’s scheme

In this section, we mainly review medical server registration phase, user registration phase, login phase, authentication and key agreement phase of Amin and Biswas’s scheme. Amin and Biswas quote bio hashing $H(\cdot)$ to resolve high false rejection [4]. Compared with modular exponentiation and elliptic curve point multiplication, bio hashing is more efficient [5].

Medical server registration phase

$MS_j$ selects its identity $ID_{ms_j}$ and sends it to medical registration server $MRS$ through a secure channel. $MRS$ calculates $X_j = h(ID_{ms_j} \| X_c)$ and submits $X_j$ to $MS_j$ via a secure channel, where $X_c$ is the master secret key of $MRS$.

User registration phase
The user \( U_i (1 < i \leq n) \) selects identity \( ID_i \), password \( PW_i \), and scans his/her biometric \( B_i \) at the sensor. Then \( U_i \) computes \( PWD_i = h(ID_i || PW_i) \) and submits the information \( \{ID_i, PWD_i, B_i\} \) to medical registration server \( MRS \) via a secure channel. On receiving the message from \( U_i \), \( MRS \) computes \( F_i = H(B_i) \); \( REG_i = h(ID_i || PWD_i) \); \( A_j = h(ID_j || X_j) \oplus REG_j \); \( P_j = h(ID_{ms_j} || X_j || F_i) \oplus h(REG_i || F_i) \) and stores the information \( \langle ID_{ms_j}, A_j, P_j \rangle \) into a table. Then \( MRS \) sends a smart card which contains \( \{ID_{ms_j}, A_j, P_j, REG_i, F_i, h(\cdot), H(\cdot)\} \) to \( U_i \) via a secure channel.

Login phase

Step 1: The user \( U_i \) inserts his/her smart card into card reader device and scans his/her biometric \( B_i \). The smart card calculates \( F_i^* = H(B_i) \) and checks if \( F_i^* = F_i \). If not, terminates it. Otherwise, the smart card asks \( U_i \) to input \( PWID_i \). Step 2: The smart card computes \( PWID_i = h(ID_i || PW_i) \); \( REG_i^* = h(ID_i || PWD_i) \), and compares whether \( REG_i^* = REG_i \). If it holds, the identity \( ID_i \) and password \( PW_i \) are valid. Then the smart card generates a random number \( cR \) and computes \( XIDhREGA = h(ID_i \oplus REG_i) \); \( RChD = cR || h(REG_i || F_i) \); \( XIDhFXIDhFREGhPE = h(ID_i || X_i || F_i || F_i) \), and stores the information \( \{ID_i, PWID_i, F_i, h(\cdot), H(\cdot)\} \) to the smart card. Then \( MRS \) sends a smart card which contains \( \{ID_{ms_j}, A_j, P_j, REG_i, F_i, h(\cdot), H(\cdot)\} \) to \( U_i \) via a secure channel.

Authentication and key agreement phase

Step 1: \( MS_j \) calculates \( E_i^* = h(ID_{ms_j} || X_j || F_i) \); \( ID_i^* = G_i \oplus E_i^* \); \( R_i^* = L_i \oplus E_i^* \); \( C_i^* = h(ID_i^* || X_j) \); \( D_i^* = h(C_i^* || R_i^*) \), and checks \( D_i^* = D_i \). If they are equal, \( U_i \) is authenticated. Otherwise, \( MS_j \) rejects the session. Then \( MS_j \) generates a random number \( R_{ms} \) and calculates \( N_j = h(ID_k || X_k || F_i) \); \( O_j = ID_j \oplus N_j \); \( S_j = h(ID_k || X_k || R_{ms}) \); \( RAN_j = R_c \oplus R_{ms} \); \( Q_j = h(ID_k || N_j || R_{ms}) \). After that, \( MS_j \) submits \( \{ID_k, O_j, S_j, Q_j, F_i, RAN_j\} \) to physician server \( PS_k \).

Step 2: \( PS_k \) computes \( N_j^* = h(ID_k || X_k || F_i) \); \( ID_j^* = O_j \oplus N_j^* \); \( R_{ms}^* = h(ID_j^* || X_k) \oplus S_j \); \( R_c^* = RAN_j \oplus R_{ms} \); \( Q_j^* = h(ID_j^* || N_j^* || R_{ms}' \); and checks \( Q_j^* = Q_j \), where \( X_k \) is a shared secret key between \( PS_k \) and \( MS_j \). If successful, \( PS_k \) authenticates \( U_i \) and accepts this request. Then \( PS_k \) generates nonce \( R_k \) and computes the session key \( SK = h(ID_k^* || ID_i^* || R_k) \); \( T_k = h(h(ID_k^* || X_k) \oplus SK) \); \( RAN_k = R_c^* \oplus R_k \); \( V_k = h(ID_k^* || X_k) \oplus R_k \). In the end, \( PS_k \) forwards the message \( \{T_k, RAN_k, V_k\} \) to \( U_i \).

Step 3: On receiving the message, \( U_i \) computes \( R_k = RAN_k \oplus R_k \); \( W_k = V_k \oplus R_k^* = h(ID_k || X_k) \); \( SK^* = h(ID_k^* || ID_i^* || R_k) \); \( T_k^* = h(W_k || SK^*) \), and checks whether \( T_k^* \) is equal to \( T_k \). If they are equal, \( PS_k \) is authenticated by \( U_i \). Otherwise, \( U_i \) rejects this session.
Weakness of Amin and Biswas’s scheme

User impersonation attacks

An attacker first steals a smart card and extracts the information \{F_i, REG_i, \{ID_{ms_i}, A_j, P_j\}\} stored in the smart card [6]. Then the attacker monitors the message \{ID_{ms_j}, ID_k, G_i\} transmitted in the public channel and seeks \(A_j, P_j\) corresponding to \(ID_{ms_j}\). The attacker computes \(E_i = P_j \oplus h(REG_i||F_i)\); \(ID_i = G_i \oplus E_i\); \(C_i = A_j \oplus REG_i\); \(D_i' = h(C_i||R_a)\); \(E_i = P_j \oplus h(REG_i||F_i)\); \(G_i = ID_i \oplus E_i\); \(L_i' = E_i \oplus R_a\), where \(R_a\) is a random number. Finally, the attacker transmits the message \{ID_{ms_j}, ID_k, F_i, D_i', G_i, L_i'\} to medical server. The attacker can be verified as a legal user.

Off-line password guessing attacks

As mentioned in user impersonation attacks, after acquiring the identity \(ID_i\) of a valid user, the attacker guesses password \(PW_i'\) and computes \(h(ID||h(ID||PW_i')) = h(ID||PWD_i')\). If \(h(ID||PWD_i') = REG_i\), the guessed \(PW_i'\) is correct.

Replay attacks

After receiving the replay message \{ID_{ms_j}, ID_k, F_i, D_i, G_i, L_i\}, \(MS_j\) computes \(D_i^* = h(C_i^* ||R_i^*)\) and figures out \(D_i^* = D_i\). The medical server \(MS_j\) cannot detect replay attacks and treats the attacker as a legal user.

Privileged insider attacks

In the user registration phase of Amin and Biswas’s scheme, a privileged insider of the server can obtain registration message \{ID_i, PW_i, B_i\}. Because of \(PW_i = h(ID||PW_i)\), the privileged insider is able to guess correct password \(PW_i\) to satisfy this equation.

Forward secrecy

In Amin and Biswas’s scheme, the attacker can compute the previous session keys once \(X_c\) is compromised. After monitoring the message \{ID_{ms_j}, ID_k, F_i, G_i, L_i, ID_k, RAN_k\} from the public channel, the attacker computes \(X_j = h(ID_{ms_j}||X_c)\); \(E_i = h(ID_{ms_j}||F_i)\); \(ID_i^* = G_i \oplus E_i\); \(R_c = L_i \oplus E_i\); \(R_k = RAN_k \oplus R_c\); \(SK = h(ID_k||D_k||R_c||R_k)\).

The proposed scheme

Step 1: \(MS_j\) submits its identity \(ID_{ms_j}\) to medical registration server \(MRS\) via a secure channel. Then \(MRS\) computes \(X_j = h(ID_{ms_j}||X_c)\) and transmits \(X_j\) to \(MS_j\) via a secure channel.

Step 2: The user \(U_i\) selects identity \(ID_i\), password \(PW_i\) and imprints his/her biometrics \(B_i\) at the sensor. Then \(U_i\) calculates \(AD_i = h(ID_i||H(B_i))\); \(AW_i = h(ID_i||PW_i||r)\), and sends the message \{\(AD_i, AW_i\}\} to \(MRS\) via a secure channel, where \(r_i\) is a random number.
Step 3: MRS computes $B_j = h(X_j||A_D)\); $C_j = B_j \oplus AW_i$, and issues a smart card containing $\{ID_{ms,j}, C_j, A_D, d(\cdot), \tau\}$ to $U_i$. Note that $d(\cdot)$ is a function that determines differences between two biometric templates that are even if belong to a same person, may have a few differences, and $\tau$ is a threshold for acceptability of this difference [7].

Step 4: Upon receiving the smart card, $U_i$ computes $A_j = h(ID_j||PW_i) \oplus H(B_j)$ and stores $\{A, r, h(\cdot), H(\cdot)\}$ into it.

Login and authentication phase

The user $U_i$ inserts the smart card into a card reader, enters $ID_i$, $PW_i$, and scans $B_i$ at the sensor.

Step 1: The smart card computes $A'_j = h(ID_j||PW_i) \oplus H(B_j)$ and checks whether $d(A'_j, A_j) < \tau$ or not. If it does hold, the smart card calculates $AW_i = h(ID_i||PW_i||j); B_j = C_j \oplus AW_i; F_i = h(B_j||4D_i||T_{ui}||ID_{ms,j}); G_j = B_j \oplus (F_j||T_{ui}||ID_{ms,j})$, where $T_{ui}$ is current timestamp. Finally, the smart card forwards the login request message $\{ID_{ms,j}, G_j, A_D\}$ to $MS_j$.

Step 2: $MS_j$ calculates $B_j' = h(X_j||A_D); F_j||T_{u_i}||ID_k = G_j \oplus B_j'$, and checks if $|T_{ms,j} - T_{ui}| \leq \Delta T$, where $T_{ms,j}$ is current timestamp. If it holds, $MS_j$ computes $F'_i = h(B_j'||AD||T_{u_i}||ID_{ms,j})$ and checks whether $F'_i = F_i$. If yes, $MS_j$ computes $H_i = h(X_k||F_i||ID_k||ID_{ms,j}); J_i = X_k \oplus (H_i||F_i||T_{ms,j})$, and submits the message $\{J_i\}$ to $PS_k$.

Step 3: Upon receiving $\{J_i\}$ at $PS_k$, $PS_k$ calculates $H_i||F_i||T_{ms,j} = J_i \oplus X_k$ and examines $|T_{ps_k} - T_{ms,j}| \leq \Delta T$ and $H_i = h(X_k||F_i||ID_k||T_{ms,j})$, where $X_k$ is shared secret key between $PS_k$ and $MS_j$. If the timestamp $T_{ps_k}$ is fresh and the equation holds, $PS_k$ computes $L_i = F_i \oplus X_k \oplus T_{ps_k}; P_i = h((X_k \oplus T_{ps_k})||F_i); SK = h(P_i||ID_k); Q_i = F_i \oplus (L_i||P_i)$. Otherwise, $PS_k$ terminates this request. Finally, $PS_k$ forwards the message $\{Q_i\}$ to $U_i$.

Step 4: $U_i$ computes $L_i||P_i = Q_i \oplus F_i; X_k \oplus T_{ps_k} = F_i \oplus L_i; P'_i = h((X_k \oplus T_{ps_k})||F_i)$, and checks whether $P'_i = P_i$. If they are equal, $U_i$ computes the session key $SK = h(P_i||ID_k)$.

Security analysis

Off-line password guessing attacks

The attacker first obtains the information $\{ID_{ms,j}, C_j, A_j, AD, d(\cdot), \tau, h(\cdot), H(\cdot)\}$ stored in the smart card and the transmitted message $ID_{ms,j}, G_j, A_D, J_i, Q_i$ in public channel. Since biometric $B_i$ is unknown for an attacker, the attacker is unable to guess the correct values of $ID_i$ and $PW_i$ to satisfy equation $A_j = h(ID_j||PW_i) \oplus H(B_j)$ or $AD_i = h(ID_i||H(B_j))$.

User impersonation attacks
To impersonate a legitimate user, an adversary selects $AW_i^*$ and computes $B_y^* = C_y \oplus AW_i^*$; $F_i^* = h(B_y^*||AD_i||T_{a_i}||ID_{m_j})$; $G_i^* = B_y^* \oplus (F_i^*||T_{a_i}||ID_{a})$, where $T_{a_i}$ is current timestamp. Then the adversary submits the message $\{ID_{m_j}, G_i^*, AD\}$ to $MS_j$. Since $B_y^* = h(X_j||AD_i) = AW_i \oplus C_y \neq AW_i \oplus C_y$, the adversary will be detected by $MS_j$.

**Server spoofing attacks**

To masquerade as a remote medical server $MS_j$, an adversary has to transmit a valid message $\{J_i = X_k \oplus (H(||F||T_{m_j})\}$ to $PS_k$. Without shared secret key $X_k$ between $PS_k$ and $MS_j$, the adversary is unable to compute correct $J_i$ and will be detected by $PS_k$.

**Replay attacks**

In our protocol, because the information $G_{ij}$ contains fresh timestamp $T_{u_i}$, login request message are different in every session. After receiving the replay message $\{ID_{m_j}, G_{ij}, AD\}$, $MS_j$ can easily detect the replay attacks by comparing $|T_{m_j} - T_{u_i}| \leq \Delta T$.

**Privileged insider attacks**

In the registration phase, a user will deliver encapsulated identity $AD_i = h(ID_i||H(B_i))$ and password $AW_i = h(ID_i||PW_i||r_i)$ to medical registration server. Since $H(B_i)$ and $r_i$ is unknown, such a process can prevent a privileged insider from acquiring user’s identity and password.

**Performance comparisons**

In order to evaluate the security performance of our scheme, we compare the two related schemes [8,3] with our scheme in Table 1. The efficiency comparison in terms of computational overhead among the related schemes and our proposed scheme is shown in Table 2. For convenience, $T_h$ and $T_m$ denote the time complexity of hash operation and modular multiplication operation, respectively. As shown in Table 1, we can see that Lu et al.’s scheme and Amin and Biswas’s scheme only withstand two out of six attacks. However, our improved scheme can achieve all the security requirements listed in Table 1. From Table 2, we can conclude that our scheme is more efficient than the other two schemes [8,3].

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password guessing attacks</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User impersonation attacks</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Server spoofing attacks</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Replay attacks</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Privileged insider attacks</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Man-in-the-middle attacks</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User anonymity</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 1. Security comparison.
Table 2. Efficiency Comparison.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Computation cost of the user</td>
<td>$6T_h + 2T_m$</td>
<td>$7T_h$</td>
<td>$6T_h$</td>
</tr>
<tr>
<td>Computation cost of the server</td>
<td>$5T_h + 2T_m$</td>
<td>$11T_h$</td>
<td>$6T_h$</td>
</tr>
</tbody>
</table>

Conclusion

In this paper, we have analyzed Amin and Biswas’s authentication scheme and demonstrated that their scheme does not fulfill their claims as it satisfies all the desirable security attributes. To remedy security flaws, we have proposed a secure biometric-based remote user authentication scheme. The security and performance analysis show that the proposed scheme not only withstands kinds of attacks but also presents efficient login and authentication phase.

Acknowledgement

This work is supported by Natural Science Foundation of Shandong Province (No.ZR2013FM009).

References


