Journal of Engineering and Applied Sciences 14 (14): 4690-4697, 2019
ISSN: 1816-949X

Security Weaknesses of Lightweight Communication Overhead Authentication Scheme using Smart Card

Younsung Choi
Major of Cyber Security, Department of Computer Science, Howon University, Gunsan-si,
54058 Jeollabuk-do, Republic of Korea

Abstract: A password-based authentication protocol is a security technology that ensures confidentiality and integrity for users who use services in a public network. Recently, Sahlani and Lu proposed a lightweight authenticated key agreement scheme using smart card and insisted that their scheme can withstand various types of attacks and satisfy diverse security requirements. However, after careful analysis, we discovered that Sahlani and Lu's authentication scheme includes several security vulnerabilities. First, the registration phase of their scheme is inefficient, since, users are using unnecessary verification process. Second, their scheme employs an improper identification process for user biometrics. Third, the scheme cannot guarantee to protect from off-line identity guessing attack and there is no session key verification process in the authentication process. In this study, we explain in detail how the aforementioned vulnerabilities occur and propose an upgraded version. The analysis shows that our proposed scheme is more secure and efficient than other related authentication schemes.

Key words: Authentication, smart card, biometric, session key verification process, analysis, Sahlani

INTRODUCTION

With the rapid development of the Information and Communication Technology (ICT), the latest technologies such as Internet of Things (IoT), big data and cloud services have brought about remarkable changes to our daily lives. Although, users enjoy the simplicity and efficiency in diverse technologies, security has emerged as a major issue in both academia and industry. In particular, it is necessary to ensure the confidentiality and integrity of data packets transmitted in the wireless environment and ensures that the users connecting to the network are legitimate users. To guarantee these security requirements, many enterprises and organizations use authenticated key agreement protocols.

Since, Lamport (1981) first proposed a password-based authentication method and many authentication researches (Hwang and Li, 2000) have been conducted to improve the security and efficiency of various environments. Hwang and Li (2000) presented a remote authentication scheme with ELGamal public key encryption technique. They insisted that their scheme is secure under replay attacks. However, Chan and Cheng (2000) proved that Hwang and Li's (2000) scheme is vulnerable to user impersonation attack. Das *et al.* (2004) proposed a dynamic ID-based remote user authentication scheme using smart card. They insisted that their scheme is safe against replay attack, forgery attack, off-line password guessing attack and privileged insider attack. However, Liao *et al.* (2005) pointed out that Das *et al.* (2004) cannot guarantee protection against off-line password guessing attack and presented an improved authentication protocol. Unfortunately, Misbahuddin and Bindu (2008) proved that the protocol (Liao *et al.*, 2005) is vulnerable to impersonation attack and reflection attack.

By Xu *et al.* (2009) presented a password-based authentication scheme using smart card. They insisted that their protocols are safe for a variety of attacks, even if the information stored in the smart card is exposed. However, by Song (2010) demonstrated that Xu *et al.* (2009) is vulnerable to user impersonation attack and then Song (2010) presented an enhanced protocol. By Sood *et al.* (2010) also found that Xu *et al.* (2009) is vulnerable to off-line password guessing attack and forgery attack and then proposed an improved scheme. Unfortunately, by Chen *et al.* (2014) proved that Song's authentication protocol (Song, 2010) overlooked stolen smart card attack. Chen *et al.* (2014) also pointed out that Sood *et al.* (2010) does not achieve mutual authentication property. Chen *et al.* (2014) then suggested an improved password based authentication scheme that solved Song's and Sood *et al.* flaws. However, by Li *et al.* (2013) discovered that Chen *et al.* (2014) cannot provide perfect forward secrecy and detect the wrong password in login phase. Besides, the password change of Chen *et al.* (2014)

Table 1: Notations

Notations	Descriptions
U_i	Remote User
S	Authentication Server
TPW_i	Temporary Password of U_i
ID_i, PW_i	Identity and Password of U_i
Bio	Biometric information of U_i
x	Master key of S
α, β	Random numbers
SK	Session Key
h(•)	One-way hash function
H(•)	Biohash function
T_u, T_s	Current Timestamps
ΔT	The maximum of Transmission delay time

is inefficient, since, the user has to communicate with the server to update his/her password. Then Li *et al*. (2013) presented an enhanced user authentication protocol.

Recently, Al Sahlani and Lu (2016) pointed out that Li *et al*. (2013) authentication protocol is vulnerable to forgery attack, user impersonation attack and server impersonation attack. In compensating for these defects, Sahlani and Lu then presented an authentication and key agreement scheme, arguing that their scheme can resist various attack types. However, we demonstrated that Al Sahlani and Lu (2016) possesses critical security vulnerabilities. Their scheme has an unnecessary verification process in registration phase, employs an improper identification process for user biometrics and cannot guarantee protection against an off-line identity guessing attack and cannot provide session key verification process. In this study, we describe in detail how previously-stated weaknesses operate and propose a more developed version.

Literature review

Review of Sahlani and Lu's scheme: In this study, we review Al Sahlani and Lu (2016). We describe each phase of Sahlani and Lu's scheme in this study and Table 1 shows the notations used in the remainder of the study.

Registration phase: The registration phase begins when a User U_i sends the registration request to S through a secure channel. Figure 1 illustrates the registration phase of Al Sahlani and Lu (2016) and the following describes this process in detail: U_i selects ID_i and TPW_i and U_i computes EID = h(ID_i||b) using random number b. U_i then sends a registration request {EID, TPW_i} to S through secure channels.

After receiving the registration request, S computes SID = h (EID||x) and checks SID. If the SID is existing value, S rejects the registration request. Otherwise, S updates the new user with SID in its database. S computes as follows.

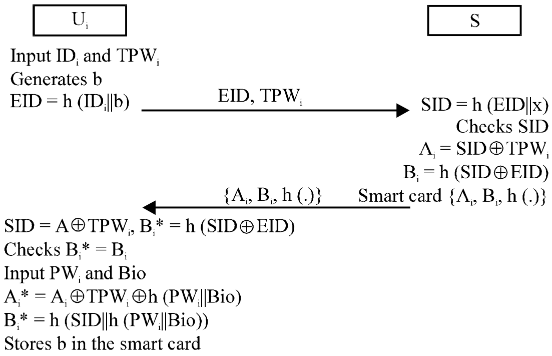


Fig. 1: Registration phase of Sahlani and Lu's scheme

$$A_i = SID \oplus TPW_i,$$
$$B_i = h(SID \oplus EID)$$

S then stores {A_i, B_i, h (•)} into a smart card and issues the smart card to User U_i through a secure channel. After receiving the smart card, U computes SID = A_i⊕TPW_i, B_i^* = h (SID⊕EID) and then checks B_i^* = B_i. U_i selects PW_i and Bio and computes as follows:

$$A_i^* = A_i \oplus TPW_i \oplus h(PW_i||Bio)$$
$$B_i^* = h\ (SID||h(PW_i||Bio))$$

U_i stores b in the smart card and replaces the existing values A_i and B_i with the new values A_i^* and B_i^*, respectively. Finally, the smart card contains the values {A_i^*, B_i^*, h (•), b}.

Login phase: The login phase begins when U_i inserts the U_i's smart card into a card reader and inputs the ID_i, PW_i and Bio. In this phase, U_i sends the login request to the Server S through the public channel. Figure 2 illustrates the login and authentication phase of Al Sahlani and Lu (2016) and the following describes this process in detail.

- U_i inserts U_i's smart card into a card reader and inputs the ID_i, PW_i and Bio
- The smart card computes:

$$SID = A_i \oplus h(TPW_i)$$
$$B_i^* = h(SID \oplus EID)$$

The smart card then verifies B_i^* = B_i. If they are not equal, the smart card terminates session, otherwise goes to the next step. U_i generates a random number α and computes:

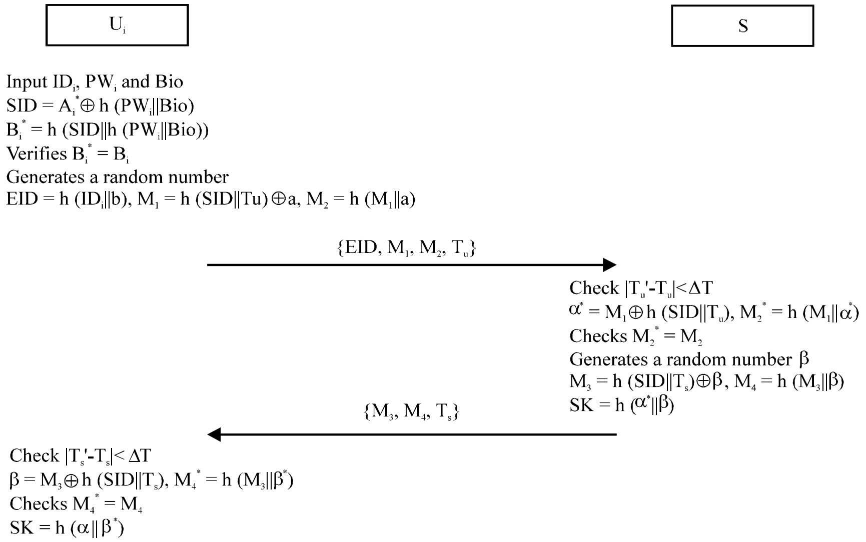

U_i
S
Input ID_i, PW_i and Bio
$SID = A_i^* \oplus h\ (PW_i||Bio)$
$B_i^* = h\ (SID||h\ (PW_i||Bio))$
Verifies $B_i^* = B_i$
Generates a random number
$EID = h\ (ID_i||b)$, $M_1 = h\ (SID||Tu) \oplus a$, $M_2 = h\ (M_1||a)$
$\{EID, M_1, M_2, T_u\}$
Check $|T_u\text{'}-T_u|<\Delta T$
$\alpha^* = M_1 \oplus h\ (SID||T_u)$, $M_2^* = h\ (M_1||\alpha^*)$
Checks $M_2^* = M_2$
Generates a random number β
$M_3 = h\ (SID||T_s) \oplus \beta$, $M_4 = h\ (M_3||\beta)$
$SK = h\ (\alpha^*||\beta)$
$\{M_3, M_4, T_s\}$
Check $|T_s\text{'}-T_s|< \Delta T$
$\beta = M_3 \oplus h\ (SID||T_s)$, $M_4^* = h\ (M_3||\beta^*)$
Checks $M_4^* = M_4$
$SK = h\ (\alpha|| \beta^*)$

Fig. 2: Login and authentication phase of Sahlani and Lu's scheme

$$EID = h\ (ID_i||b),$$
$$M_1 = h\ (SID||T_u) \oplus \alpha,\ M_2 = h(M_1||\alpha)$$

U_i then sends the login request message {EID, M_1, M_2, T_u} to Server S through a public channel.

Authentication phase: When the Server S receives the login request message from the user U_i, the authentication phase begins and the following describes this process in detail.

After receiving the login request message, S verifies, whether the SID = h (EID||x) is a legitimate value of User U_i. Then, it checks if $(T_u\text{'}-T_u) \leq \Delta T$. If $(T_u\text{'}-T_u) \leq \Delta T$, then, the next step proceeds; otherwise, this phase is terminated. The S computes $\alpha^* = M_1 \oplus h\ (SID||T_u)$ and $M_2^* = h\ (M_1||\alpha^*)$ and then checks $M_2^* = M_2$. If this is satisfied, the S accepts the login request; otherwise, the login request is rejected and this phase is terminated. S generates a random number α and computes:

$$M_3 = h(SID||T_s) \oplus \beta,\ M_4 = h(M_3||\beta)$$
$$SK = h(\alpha^*||\beta)$$

Then, S sends the authentication request {M_3, M_4, T_s} to user U_i. After receiving the authentication request, U_i checks the Timestamp T_s in the received message with the condition $(T_s\text{'}-T_s) \leq \Delta T$. If $(T_s\text{'}-T_s) \leq \Delta T$, U_i accepts the authentication request; otherwise, the authentication request is rejected and this phase is terminated. The user U_i computes $\beta^* = M_3 \oplus h\ (SID||T_s)$ and $M_4^* = h\ (M_3||\beta^*)$ and then checks the equation $M_4^* = M_4$. If there are satisfied, U_i accepts the S; otherwise, it rejects the S. Finally, U_i computes the shared session key $SK = h(\alpha||\beta^*)$.

Password change phase: The password change phase begins when user U_i wants to change his/her Password PW_i with a new Password PW_i^{new}. Figure 3 illustrates the password change phase of Al Sahlani and Lu (2016): U_i inserts U_i's smart card into a card reader and inputs the ID_i, PW_i and Bio; the smart card computes:

$$SID = A_i^* \oplus h\ (PW_i||Bio)$$
$$B_i^* = h\ (SID||h\ (PW_i||Bio))$$

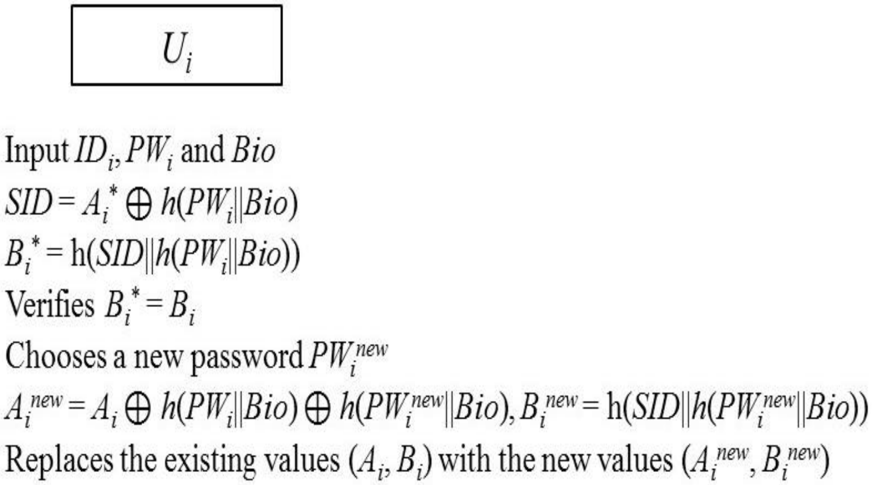
The smart card then verifies $B_i^* = B_i$. If they are not equal, the smart card terminates session, otherwise goes to the next step.

U_i chooses a new Password PW_i^{new}. Then, the smart card computes $A_i^{new} = A_i \oplus h\ (PW_i||Bio) \oplus h\ (PW_i^{new}||Bio)$ and $B_i^{new} = h\ (SID||h\ (PW_i^{new}||Bio))$. The smart card replaces the existing values (A_i, B_i) with the new values (A_i^{new}, B_i^{new}).

Weaknesses of Sahlani and Lu's scheme: In this study, we describe that Al Sahlani and Lu (2016) possesses several security weaknesses. The following weaknesses are based on the two assumptions that:

- An attacker can extract all information stored in the smart card by physically monitoring its power consumption (Jung *et al*., 2017; Choi *et al*., 2016)
- An attacker can intercept or transform any messages in the public channel (Jung *et al*., 2016, 2017; Jaewook *et al*., 2017)

Under these two assumptions, the following problems have been found and their detailed descriptions are given as follows:



U_i

Input ID_i, PW_i and Bio

$SID = A_i^* \oplus h(PW_i \| Bio)$

$B_i^* = \mathrm{h}(SID \| h(PW_i \| Bio))$

Verifies $B_i^* = B_i$

Chooses a new password PW_i^{new}

$A_i^{new} = A_i \oplus h(PW_i \| Bio) \oplus h(PW_i^{new} \| Bio), B_i^{new} = \mathrm{h}(SID \| h(PW_i^{new} \| Bio))$

Replaces the existing values (A_i, B_i) with the new values (A_i^{new}, B_i^{new})

Fig. 3: Password change phase of Sahlani and Lu's scheme

Unnecessary verification process: In the registration phase of Sahlani and Lu's scheme, after receiving the smart card from the Server S, U_i computes:

$$\mathrm{SID} = \mathrm{A_i} \oplus \mathrm{TPW_i}$$
$$\mathrm{B_i^*} = \mathrm{h}(\mathrm{SID} \oplus \mathrm{EID})$$

U_i, then, conducts a verification procedure through $B_i^* = B_i$. This verification is a procedure to verify that the server issuing the smart card is a legitimate server. However, since, the registration phase is performed in a secure channel, a separate verification procedure is not required. Thus, this verification process results in unnecessary computational waste.

Biometric identification problem: The user's biometric information is very sensitive data. Thus, when user identification is carried out using biometric data, a secure and sophisticated matching technique is required. During the login phase of Sahlani and Lu's scheme, U_i inserts U_i's smart card into a card reader and inputs the ID_i, PW_i and Bio. After computing SID = $A_i^* \oplus$h ($Pw_i \|$Bio) and B_i^* = h (SID$\|$h($PW_i \|$Bio)), the smart card performs the verification process through $B_i^* = B_i$.

However, their scheme can cause problems in that the user's biometric information is simply computed by using a one-way hash function. That is the B_i value computed at the registration phase and the B_i^* value computed at the login phase are very different from each other, since, if the input values of the one-way hash function are slightly different, the output values will produce completely different results. Accordingly, there is a high probability that the verification procedure comparing B_i^* and B_i will not be performed properly.

Off-line identity guessing attack: Generally, the identity of the user used in the authentication protocol is one of secret information that should not be exposed (Jung *et al*., 2016). However, by Al Sahlani and Lu (2016), the attacker can obtain the user's ID_i through the off-line guessing attack. The following is a detailed description of the attack scenario:

Step 1: After an attacker has stolen the smart card, attacker can extract {A_i^*, B_i^*, h(•), b} in U_i's smart card.

Step 2: Attacker can use the eavesdropped login request message {EID, M_1, M_2, T_u} from the public channel.

Step 3: Attacker selects a password candidate ID_a.

Step 4: Attacker computes EID_a = h ($ID_a \|$b).

Step 5: The attacker repeats above steps from 3-4 until the computed result EID_a equals the eavesdropped value EID.

Step 6: If they correspond with each other, ID_a would be the accurate identity. If not, the attacker repeats the above steps until finding the correct identity.

Therefore, the aforementioned descriptions, an attacker can acquire the user's identity ID_i and can know who is performing the key agreement protocol with the Server S.

Absence of a session key verification process: According to Blake *et al*. (1997) and Islam *et al*. (2015), the authenticated key agreement protocol recommends an authentication procedure to verify the coherence of the generated session keys between a user and a server.

However, in Sahlani and Lu's scheme, a user makes his/her own session key after verifying the authentication request message without a coherence test. That is to say, the user can hardly be sure whether the new generated session key is correct or not.

In order to ensure an accurate session key distribution between a user and a server, the following procedures are required: after generating a session key, the server sends an authentication request including this session key's information, the user should guarantee the accuracy of the session key from the server, verifying the received authentication request message.

MATERIALS AND METHODS

Proposed scheme: In this study, we suggest a security enhanced authentication and key agreement scheme to overcome the security weaknesses by Al Sahlani and Lu (2016). Our proposed scheme also consists of four phases: a registration, login, authentication and password change. The notation in our scheme is summarized in Table 1.

Registration phase: The registration phase begins when a user U_i sends the registration request to S through a secure channel. Figure 4 illustrates the registration phase of the proposed scheme and the following describes this process in detail.

- U_i selects ID_i, PW_i and imprints user's biometric information Bio. U_i computes $RPW_i = h(PW_i \| H(Bio))$ using biohash function H (•) and sends a registration request $\{ID_i, RPW_i\}$ through a secure channel
- The S computes $A_i = h(ID_i \| RPW_i)$ and $B_i = A_i \oplus x$. The S erver S stores $\{B_i$, h (•), H (•)$\}$ into a smart card and issues this smart card to user U_i through a secure channel
- The U_i computes $C_i = h(Id_i \| PW_i \| H(Bio))$ and stores the C_i into the card. Finally, the smart card contains $\{B_i, C_i$, h (•), H(•)$\}$

Login phase: The login phase begins when U_i inserts the U_i's smart card into a card reader and inputs the ID_i, PW_i and Bio. In this phase, U_i sends the login request to the Server S through the public channel. Figure 5 illustrates the login and authentication phase of the proposed scheme and the following describes this process in detail.

U_i inserts U_i's smart card into a card reader and inputs the ID_i, PW_i and Bio. U_i computes $C_i' = h(Id_i \| PW_i \| H(Bio))$ and compares C_i' with the stored value C_i. If this condition is hold, the smart card acknowledges the legitimacy of the U_i and proceeds with the next step. Otherwise, it terminates this phase.

U_i generates a random number α and computes $RPW_i = h(Pw_i \| H(Bio))$, $A_i = h(ID_i \| RPW_i)$, $EID_i = ID_i \oplus A_i$, $M_1 = ID_i \oplus \alpha$ and $M_2 = h(Id_i \| A_i \| \alpha)$. Finally, the U_i sends login request message $\{EID_i, B_i, M_1, M_2, T_u\}$ to Server S.

Authentication phase: When the Server S receives the login request message from the User U_i, the authentication phase begins and the following describes this process in detail.

After receiving the login request message, S checks the validity of timestamp $(T_u' - T_u) \leq \Delta T$. S, then, computes $Id_i' = EID_i \oplus B_i \oplus x$, $\alpha' = M_1 \oplus ID_i'$ and $M_2' = h(Id_i' \| B_i \oplus x \| \alpha')$ and compares M_2' with the received value M_2. If this condition is hold, the procedure goes to the next step. Otherwise, this phase is terminated.

The S generates a random number β and computes $SK = h(\alpha' \| \beta)$, $M_3 = \beta \oplus h(\alpha' \| M_2')$ and $M_4 = h(M_2' \| SK)$. The S, then, sends the authentication message $\{M_3, M_4, T_s\}$ to U_i.

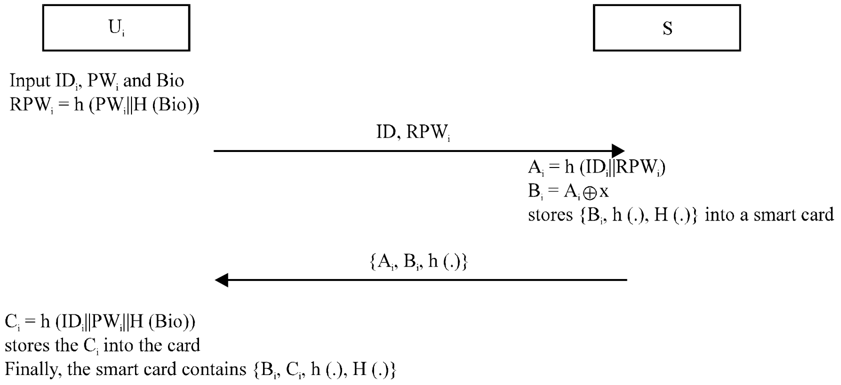

U_i
S
Input ID_i, PW_i and Bio
RPW_i = h (PW_i||H (Bio))
ID, RPW_i
A_i = h (ID_i||RPW_i)
B_i = A_i⊕x
stores {B_i, h (.), H (.)} into a smart card
{A_i, B_i, h (.)}
C_i = h (ID_i||PW_i||H (Bio))
stores the C_i into the card
Finally, the smart card contains {B_i, C_i, h (.), H (.)}

Fig. 4: Registration phase of the proposed scheme

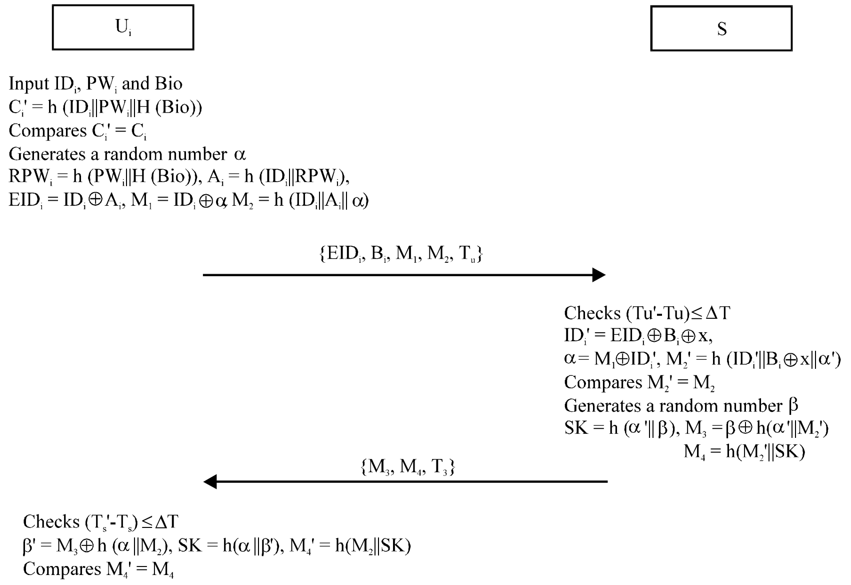
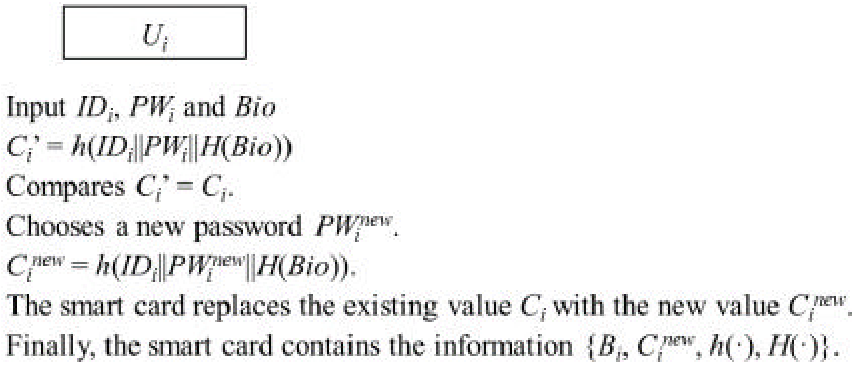

U_i
S
Input ID_i, PW_i and Bio
$C_i' = h(ID_i||PW_i||H(Bio))$
Compares $C_i' = C_i$
Generates a random number α
$RPW_i = h(PW_i||H(Bio))$, $A_i = h(ID_i||RPW_i)$,
$EID_i = ID_i \oplus A_i$, $M_1 = ID_i \oplus \alpha$ $M_2 = h(ID_i||A_i||\alpha)$
$\{EID_i, B_i, M_1, M_2, T_u\}$
Checks $(Tu'-Tu) \leq \Delta T$
$ID_i' = EID_i \oplus B_i \oplus x$,
$\alpha = M_1 \oplus ID_i'$, $M_2' = h(ID_i'||B_i \oplus x||\alpha')$
Compares $M_2' = M_2$
Generates a random number β
$SK = h(\alpha'||\beta)$, $M_3 = \beta \oplus h(\alpha'||M_2')$
$M_4 = h(M_2'||SK)$
$\{M_3, M_4, T_3\}$
Checks $(T_s'-T_s) \leq \Delta T$
$\beta' = M_3 \oplus h(\alpha||M_2)$, $SK = h(\alpha||\beta')$, $M_4' = h(M_2||SK)$
Compares $M_4' = M_4$

Fig. 5: Login and authentication phase of the proposed scheme



U_i

Input ID_i, PW_i and Bio
$C_i' = h(ID_i||PW_i||H(Bio))$
Compares $C_i' = C_i$.
Chooses a new password PW_i^{new}.
$C_i^{new} = h(ID_i||PW_i^{new}||H(Bio))$.
The smart card replaces the existing value C_i with the new value C_i^{new}.
Finally, the smart card contains the information $\{B_i, C_i^{new}, h(\cdot), H(\cdot)\}$.

Fig. 6: Password change phase of proposed scheme

After receiving the authentication request, U_i checks the Timestamp T_s in the received message with the condition $(T_s'–T_s) = \Delta T$. The U_i computes $\beta' = M_3 \oplus h(\alpha||M_2)$, $SK = h(\alpha||\beta')$ and $M_4' = h(M_2||SK)$ and compares M_4' with the received value M_4. If this condition is hold, U_i acknowledges the legitimacy of the S; otherwise, it terminates this phase.

Password change phase: The password change phase begins when User U_i wants to change his/her Password PW_i with a new Password PW_i^{new}. Figure 6 illustrates the password change phase of the proposed scheme.

U_i inserts U_i's smart card into a card reader and inputs the ID_i, PW_i and Bio. U_i Computes $C_i' = h(ID_i||PW_i||H(Bio))$ and Compares C_i' with the stored value C_i. If this condition is hold, the smart card acknowledges the legitimacy of the U_i and proceeds with the next step. Otherwise, it terminates this phase. U_i chooses a new password PW_i^{new}. Then, the smart card computes $C_i^{new} = h(ID_i||PW_i^{new}||H(Bio))$.

The smart card replaces the existing value C_i with the new value C_i^{new}. Finally, the smart card contains the information $\{B_i, C_i^{new}, h(\bullet), H(\bullet)\}$.

RESULTS AND DISCUSSION

Security analysis: In this study, we evaluate whether the proposed scheme is safe for various types of attacks and satisfies various security requirements. Table 2 shows a security comparison of our scheme and other related schemes (Liao *et al*., 2005; Misbahuddin and Bindu, 2008; Xu *et al*., 2009). The detailed description is as follows.

Table 2: Security comparison of the proposed scheme and other related schemes

Features	Chen *et al.* (2014)	Li *et al.* (2013)	Sahlani and Lu (2016)	Proposed schemes
Efficient registration phase	Yes	Yes	No	Yes
Provide mutual authentication	Yes	Yes	Yes	Yes
Resistance to off-line password guessing attack	No	No	Yes	Yes
Resistance to off-line identity guessing attack	Yes	Yes	No	Yes
Provide proper biometric identification	-	-	No	Yes
Resistance to insider attack	No	No	Yes	Yes
Provide session key verification process	No	No	No	Yes
Resistance to replay attack	Yes	Yes	Yes	Yes

Efficient registration phase: In Sahlani and Lu's protocol, the user performed unnecessary verification procedures when registering with the server. However, in our protocol, the efficiency of the registration phase has been improved by eliminating the procedure for the User U_i to verify the Server S.

Provide mutual authentication: In our scheme, the S can authenticate the user by checking whether the login request is correct $\{EID_i, B_i, M_1, M_2, T_u\}$. In addition, the U_i can also authenticate the S by checking whether the authentication message $\{M_3, M_4, T_s\}$ is correct.

Resistance to off-line password guessing attack: In our scheme, an attacker can obtain from the stolen smart card $\{B_i, C_i, h (\bullet), H (\bullet)\}$ and intercept the login request message $\{EID_i, B_i, M_1, M_2, T_u\}$. Using these values, the attacker may try to guess the correct Password PW_i. However, without knowing ID_i and H (Bio), the attacker cannot guess PW_i. In addition, H (Bio) is hashed biometric information which is only known by U_i. Thus, the proposed scheme is secure against off-line password guessing attacks.

Resistance to off-line identity guessing attack: To guess the user's ID_i, the attacker must know either the random number α or the server's secret value x. However, in our scheme it is impossible to know the random number α and the secret value x.

Provide proper biometric identification: In contrast with Sahlani and Lu's scheme, our scheme uses a bio-hashing technique in order to provide an accurate user identification process. In the login phase, after U_i inputs his/her U_i and PW_i and imprints biometric Bio, the smart card computes $C_i' = h (Id_i||PW_i||H (Bio))$ and Compares C_i' with the stored C_i value in the smart card. Therefore, our scheme can prevent a biometric matching error and provides a proper identification process.

Resistance to insider attack: In our proposed scheme, the U_i sends the password information to S in the form of $h (PW_i||H (Bio))$ instead of the form PW_i. Accordingly, the inside attacker is unable to acquire the user's password Pw_i.

Provide session key verification process: In our scheme, generating a session key $SK = h (\alpha'||\beta)$ and the value $M_3 = \beta \oplus h (\alpha'||M_2')$ and $M_4 = h (M_2'||SK)$, a server S sends $\{M_3, M_4, T_s\}$ to user U_i. U_i computes a session key $SK = h (\alpha||\beta')$ and $M_4' = h (M_2||SK)$ and measures the coherence between M_4' and M_4 to verify the received authentication request. Since, M_4 includes the information of Session Key SK generated by S, U_i may be sure that S's Session key is accurate if the comparison results are correct.

Resistance to replay attack: An attacker can intercept data packets and try to resend it to server in order to launch the replay attack. However, the login request message of our proposed scheme includes a current timestamp such as T_u of $\{EID_i, B_i, M_1, M_2, T_u\}$. Hence, the proposed scheme can withstand against replay attack.

CONCLUSION

Recently, Sahlani and Lu proposed a lightweight communication overhead authentication scheme using smart card and demonstrated that their scheme can resist various kinds of attacks including off-line password guessing attack, impersonation attack and insider attack. However, in this study, we have discovered that Sahlani and Lu's authentication scheme has an unnecessary verification process and uses an improper identification process for user biometrics. In addition, we have found that their scheme is vulnerable to off-line identity guessing attack. In order to overcome these defects, we propose an improved authentication and key agreement scheme. Our proposed scheme has been assessed with respect to various security features and we conclude that the proposed scheme properly considers efficiency and robustness.

ACKNOWLEDGEMENT

This research was supported by the National Research Foundation of Korea grant funded by Korea Government (Ministry of Science, ICT and Future Planning) (NRF-2017R1C1B5017492) and this research was supported by financial support of Howon University in 2018.

REFERENCES

Al Sahlani, A.Y.F. and S. Lu, 2016. Lightweight communication overhead authentication scheme using smart card. Indonesian J. Electr. Eng. Comput. Sci., 1: 597-606.

Blake, W.S., D. Johnson and A. Menezes, 1997. Key Agreement Protocols and their Security Analysis. In: Cryptography and Coding, Michael, D. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-63927-5, pp: 30-45.

Chan, C.K. and L.M. Cheng, 2000. Cryptanalysis of a remote user authentication scheme using smart cards. IEEE. Trans. Consum. Electron., 46: 992-993.

Chen, B.L., W.C. Kuo and L.C. Wuu, 2014. Robust smart-card-based remote user password authentication scheme. Intl. J. Commun. Syst., 27: 377-389.

Choi, Y., Y. Lee and D. Won, 2016. Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction. Intl. J. Distrib. Sens. Networks, 12: 1-16.

Das, M.L., A. Saxena and V.P. Gulati, 2004. A dynamic ID-based remote user authentication scheme. IEEE Trans. Consumer Elect., 50: 629-631.

Hwang, M.S. and L.H. Li, 2000. A new remote user authentication scheme using smart cards. IEEE Trans. Consumer Elect., 46: 28-30.

Islam, S.H., M.K. Khan and X. Li, 2015. Security analysis and improvement of a more secure anonymous user authentication scheme for the integrated EPR information system. PloS. One, 10: e0131368-e0131368.

Jaewook, J., K. Dongwoo, L. Donghoon and W. Dongho, 2017. An improved and secure anonymous biometric-based user authentication with key agreement scheme for the integrated EPR information system. PloS One, 12: 1-26.

Jung, J., J. Kim, Y. Choi and D. Won, 2016. An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks. Sens., 16: 1-30.

Jung, J., J. Moon, D. Lee and D. Won, 2017. Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks. Sens., 17: 1-21.

Lamport, L., 1981. Password authentication with insecure communication. Commun. ACM, 24: 770-772.

Li, X., J. Niu, M.K. Khan and J. Liao, 2013. An enhanced smart card based remote user password authentication scheme. J. Network Comput. Appl., 36: 1365-1371.

Liao, I.E., C.C. Lee and M.S. Hwang, 2005. Security enhancement for a dynamic ID-based remote user authentication scheme. Proceedings of the International Conference on 2005 Next Generation Web Services Practices (NweSP'05), August 22-26, 2005, IEEE, Seoul, South Korea, Korea, pp: 1-4.

Misbahuddin, M. and C.S. Bindu, 2008. Cryptanalysis of Liao-Lee-Hwangs dynamic ID scheme. Intl. J. Network Secur., 6: 211-213.

Song, R., 2010. Advanced smart card based password authentication protocol. Comput. Stand. Interfaces, 32: 321-325.

Sood, S.K., A.K. Sarje and K. Singh, 2010. An improvement of Wang *et al.*'s authentication scheme using smart cards. Proceedings of the 2010 National Conference on Communications (NCC), January 29-31, 2010, IEEE, Chennai, India, ISBN: 978-1-4244-6383-1, pp: 1-5.

Xu, J., W.T. Zhu and D.G. Feng, 2009. An improved smart card based password authentication scheme with provable security. Comput. Stand. Interfaces, 31: 723-728.