JDCS 디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 19, No. 12, pp. 2415-2422, Dec. 2018

보안성이 향상된 익명보장 두 가지 요소 상호인증 및 키 동의 기법

최 윤 성
호원대학교 컴퓨터학부 사이버보안전공

Security Enhanced Anonymous Two Factor Mutual Authentication Scheme with Key Agreement

Younsung Choi
Major of Cyber Security, Division of Computer, Howon University, Gunsan-si, 54058, Korea

[요　약]

세션 개시 프로토콜의 보안성을 향상시키고, 패스워드 기반의 기법들은 일반적으로 오프라인 패스워드 공격에 취약하다는 특징을 해결하기 위해서 두 가지 요소 상호 인증 기법에 대한 연구를 진행하고 있다. Lu 등은 타원곡선 암호를 기반으로 한 익명성과 키 동의를 제공하는 세션 게시 프로토콜을 두 가지 요소 인증 기법으로 제안하였지만, 몇 가지 보안상의 문제점이 있었다. Reddy 등은 Lu 등이 제안한 기법의 문제점을 지적하고 보다 보안성이 향상되고 익명성이 보장되는 두 가지 요소 상호 인증 기법을 제안하였다. Reddy 등이 제안한 인증 기법에도 다양한 보안 취약점이 발견되었다. 본 논문에서 Reddy 등이 제안한 기법의 동작과정을 분석하고 안전한 인증기법을 제안하고자 한다. 제안하는 인증 기법은 Reddy 등이 제안한 기법에서 발견된 오프라인 패스워드 추측 공격, DoS 공격, 잘못된 패스워드 변경, 세션키 노출 공격 등을 포함한 다양한 보안 문제점을 퍼지 추출 기술을 활용하여 해결하였다. 본 논문에서 제안하는 기법은 기존의 기법보다 보안성이 향상되고 키 동의를 제공하며 익명성이 보장되는 두 가지 요소 상호인증 기법이다.

[Abstract]

Various researcher study two-factor authentication schemes for the session initiation protocol for enhancing security, it is reason that password-based authentication schemes have security limitation on off-line password attack. Lu et al. suggested two-factor authentication scheme. it uses elliptic curve cryptography and provides the anonymity and key agreement for session initiation protocol but has security problems. Reddy et al. found out Lu et al.' scheme's vulnerability and proposed an enhanced anonymous two-factor mutual authentication with key-agreement scheme for session initiation protocol. However, their scheme has security vulnerability, so this paper executes the operation process analysis of Reddy et al.' authentication scheme. This paper proposed the security enhanced anonymous two factor mutual authentication scheme with key agreement scheme to protecting off-line password guessing attack, DoS attack, wrong password change phase, and session key disclosure attack using biometrics's fuzzy extraction.

색인어 : 안전성 분석, 세션 개시 프로토콜, 사용자 인증 기법
Key word : Security analysis, Session initiation protocol, User authentication scheme

http://dx.doi.org/10.9728/dcs.2018.19.12.2415

Received 03 December 2018;**Revised** 13 December 2018
Accepted 23 December 2018

***Corresponding Author; Younsung Choi**

Tel: +82-63-450-7476
E-mail: yschoi@howon.ac.kr

Ⅰ. Introduction

Session Initiation Protocol(known as SIP) is the important communications scheme to control multimedia communication sessions. SIP is a text-based protocol, incorporating various elements of the hypertext transfer protocol and the simple mail transfer protocol. SIP can alter, establish and terminate the connection between various communication parties. SIP is made for application layer protocol and it is designed to be independent of the underlying transport layer.[1]

SIP is involved for the signaling operations of communication session and is primarily used to set up and terminate voice or video calls. SIP can use to establish two-party or the multi-party sessions. And SIP is text- based protocol. It is used for requests from clients and responses from the servers over the public communication. Rosenberg et al. proposed the authentication scheme using SIP with challenge -response protocol in 2002. Various studies show more efficient and secure authentication schemes for SIP after Rosenberg et al.'s scheme proposed.[2]

Lu et al. proposed anonymous two-factor based authenticated key agreement scheme using elliptic curve cryptography for SIP.[3] They shows security analysis on various against attacks and provides anonymity. But Reddy et al. found out that Lu et al.' scheme has weak problems on imperfect mutual authentication and extraction of sensitive information, and in not secure to user impersonation attacks. And Reddy et al. proposed security enhanced elliptic curve cryptography based scheme. Their scheme provide anonymous two-factor mutual user authentication with key agreement scheme for SIP. Reddy et al. shows security analysis on the mutual authentication, user anonymity, perfect forward secrecy and is more secure on various attacks than various authentication schemes including Lu et al.'s scheme.[4] In this paper, first paper analyze authentication phases of Reddy et al.' authentication scheme. And Reddy et al.' scheme have security vulnerabilities such as off-line password guessing attack, a DoS attack, wrong password change phase, and session key disclosure attack. And then, this paper propose security enhanced authentication scheme.

This paper is organized as follows. Section 2 reviews the Reddy et al.'s authentication scheme. Section 3 analyzes the vulnerabilities regard as security problem in Reddy et al.'s authentication scheme. Section 4 proposes security enhanced authentication scheme, and section 5 executes security analysis on proposed scheme including the Lu et al. and Reddy et al.' authentication scheme. Section 6 concludes the paper.

Ⅱ. Review of Reddy et al.' s Scheme

This section reviewed Reddy et al.'s scheme of the registration and authentication phase.[4, 5] Notations of this paper are listed the Table 1.

Table 1. Notations

Notation	Description
U	A User
S	A server
ID_U	Identity of U
PW_U	Password of U
SC	Smartcard of U
r_U , a	Random numbers chosen by U
Pri_S	Private key of S
Pub_S	Public key of S
r_S, β	Random numbers chosen by S
P	A point on the elliptic curve
SK	Session key
$\|\|$	The concatenation operation
$h(\bullet)$	A secure one-way hash function
$\oplus$	An exclusive-OR operation

In the system initialization phase of Reddy et al.' scheme, Before the protocol is ever executed, Reddy et al.' scheme computes and shares the secret. S generates a point P on an elliptic curve $E(a, b)$ over $F_{p.}$ S selects $h(\bullet)$ and Pri_S , and calculates $Pub_S = Pri_S \bullet P$. S stores Pri_S and publishes { $E(a, b)$, P, Pub_S, $h(\bullet)$ }.

2-1 User registration phase

This phase is performed once when user U registers with the server. User U selects ID_U, PW_U, and two random numbers r_U and r. And then smart catd computes $PID_U = h(ID_U \| r_U)$, $RPW = h(PW_U \| r_U) \oplus r$. And U sends the registration request { ID_U , RPW } to S using a further secure communication. Server S computes M, N as follows. $M = h(PID_U \| ID_S \| k)$, $N = M \oplus RPW$. And then, server S puts {N, P, Pub_S , $h(\bullet)$ } on user U's smart card SC and send it to U. user U computes V_1, N', V_2 as follows. $V_1 = r_U \oplus h(ID_U \| PW_U)$, $N' = N_r = M \oplus h(PW_U \| r_U)$, $V_2 = h(PID_U \| h(PW_U \| r_U))$, And then, the U stores them on the received SC. SC includes the values {N', V_1, V_2, P, Pub_S , $h(\bullet)$}. Figure 1 shows user registration phase of Reddy et al.'s Scheme.

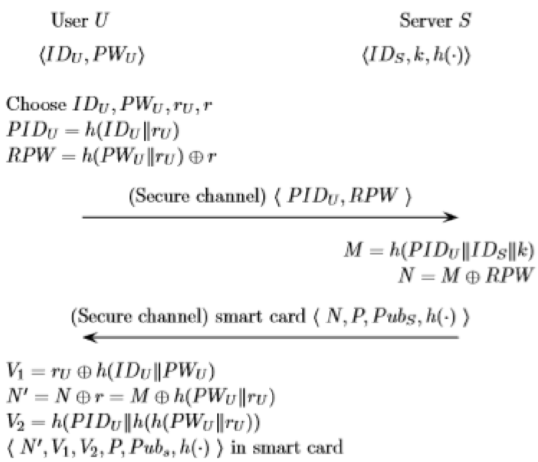

Fig. 1. User registration phase of Reddy et al.'s Scheme

2-2 Key agreement authentication phase

Figure 2 shows Key agreement authentication phase of Reddy et al.'s scheme. User U and server S can authenticate each other and compute a session key in mutual authentication with key agreement. U inputs smart card SC and inputs own ID_U and PW_U. SC computes r_U, PID_U. $r_U = V_1 \oplus h(ID_U \| PW_U)$, $PID_U = h(ID_U \| r_U)$, and checks the accuracy $V_2 \oplus h(PID_U \| h(PW_U \| r_U))$.

If they are same, then the smart card SC generates a random number a and computes N_U, M, Y as follows. $N_U = a \cdot P$, $N`_U = a \cdot Pub_S$, $M = N' \oplus h(PW_U \| r_U)$, $Y = h(PID_U \| N_U \| M)$, And then, user $U$ sends the REQUEST( $AID_U$ , $N_U$ , $Y$ ) to server $S$. $S$ computes $N`_U$, PID_U , M as follows. $N`_U = Pri_S \cdot N_U$ , $PID_U = AID_U \oplus N`_U$, $M = h(PID_U \| ID_S \| k)$, And then, verifies $Y = h(PID_U \| N_U \| M)$.

If they are same, server S authenticates U. if not, process stops. S generates a random number β and calculate X, N_S, SK_S, $auth_S$. $X = M \oplus \beta$, $N_S = \beta \cdot N`_U$, $SK_S = h(PID_U \| N_S \| \beta)$, $auth_S = h(SK_S \| PID_U \| M)$, And then, server $S$ sends *CHALLENGE*(*realm*, $X$, $auth_S$ ) to user $U$. Then using receiving *CHALLENGE* messages, $SC$ computes $\beta$, $N`_S$, SK_U as follows. $\beta = M \oplus X$, $N`_S = \beta \cdot N`_U$, $SK_U = h(PID_U \| N`_S \| \beta)$, And then, the server S verifies $auth_S$ messages as follows. $auth_S = h(SK_U \| PID_U \| M)$. If $auth_S$ is same to $h(SK_U \| PID_U \| M)$, U authenticates S and further computes $auth_U$. $auth_U = h(SK_U \| PID_U \| \beta)$, And then, U sends the *RESPONSE*(*realm*, $auth_U$) to server S. Server S checks $auth_U = h(SK_S \| PID_U \| \beta)$. If they are same, S accepts for next communication using computed session key $SK_U = SK_S$. If not, S drops the session key and stop the communication with U.

$SK_U = h(PID_U \| N`_S \| \beta)$,

$SK_S = h(PID_U \| N_S \| \beta)$.

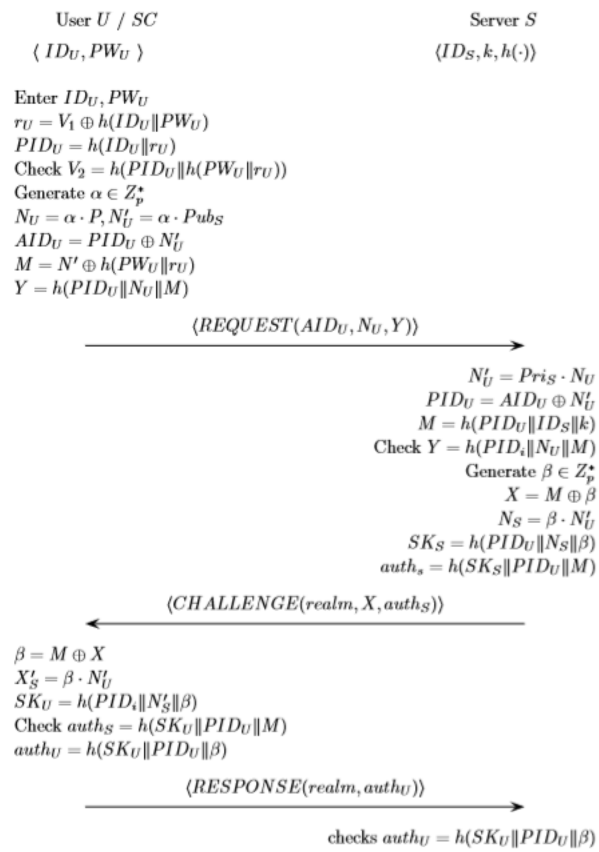

Fig. 2. Key agreement authentication phase of Reddy et al.'s Scheme

2-3 Password changing phase

Reddy et al.'s protocol claims that users can freely update user's passwords. The password change phase works as follows. U inserts SC and enters the existing user's ID_U and PW_U. SC computes r_U. $r_U = V_1 \oplus h(ID_U \| PW_U)$. And SC checks calculated value and V_2 as follows. $V_2 = h(PID_U \| h(PW_U \| r_U))$. If $V_2 = h(PID_U \| h(PW_U \| r_U))$ are corresponding, then U derives M as follows. $M = N' \oplus h(PW_U \| r_U)$. A user U selects a new password PW_{Unew} and computes RPW^{new}, V_1^{new}, N'^{new}, V_2^{new} as follows. $RPW^{new} = h(PW_U^{new} \| r_U) \oplus r$, $V_1^{new} = r_U \oplus h(ID_U \| PW_U^{new})$, $N'^{new} = M \oplus h(PW_U^{new} \| r_U)$, $V_2^{new} = h(PID_U \| h(PW_U^{new} \| r_U))$. Then, S replaces existing values on the received SC. Thus, SC contains $\{N'^{new}, V_1^{new}, V_2^{new}, P, Pub_S, h(\cdot)\}$.

Ⅲ. Security Problem on Reddy et al.' s

This paper found out that Reddy et al.' scheme have security vulnerabilities such as off-line password guessing attack, a DoS attack, wrong password change phase, session key disclosure.

3-1 Off-line Password Guessing Attack

An attacker can reveal user's identity and password from user's smart card in Reddy et al.'s authentication scheme. the attacker can analyze the stored information of smart card using the simple power analysis or differential power analysis.[7-9] If the attacker steals the user's smart card, and then the attacker obtains the all of information $\{N', V_1, V_2, P, Pub_s, h(\bullet)\}$ from smart card using physical monitoring. So the attacker can knows formula of all parameters such as V_2, PID_U and r_U.

$V_2 = h(PID_U \| h(PW_U\|r_U)$,

$PID_U = h\oplus(ID_U\|r_U)$, $r_U = V_1\oplus h(ID_U\|PW_U)$.

The attacker can compute $V_2=h(PID_U\| h(PW_U \|r_U)$ as follows. Using $PID_U \rightarrow V_2=h(h(ID_U \|r_U)\|h(PW_U\|r_U)$, Using $r_U \rightarrow V_2 = h(h(ID_U\| V_1\oplus h(ID_U\|PW_U))\|h(PW_U\|V_1 h(ID_U\|PW_U))$.

The attacker got $V_1, V_2, h(\bullet)$ from U's SC, and so does not know ID_U and PW_U on $V_2 = h(h(ID_U \|V_1\oplus h(ID_U\|PW_U))\|h(PW_U\|V_1\oplus h(ID_U\| PW_U))$. The attacker can guess the ID_U and PW_U because they are both small size. $|D_{id}|$ and $|D_{pw}|$ defined the number of identities in D_{id} and the number of passwords in D_{pw}. If T_H is the running time for hash funtion, the running time of the aforementioned attack procedure is $|D_{id}| * |D_{pw}| * T_H)$, because both PW and ID are human-memorable short strings but not high-entropy keys. So $|D_{id}|$ and $|D_{pw}|$ are often chosen from two corresponding dictionaries of small size. As $|D_{id}|$ and $|D_{pw}|$ are very limited in practice, $|D_{id}|\leq |D_{pw}| \leq 10^6$, the aforementioned attack can be completed inpolynomial time. Therefore the attacker can ID_U and PW_U using off-line password (and identity) guessing attack on Reddy et al.'s authentication scheme.

3-2 DoS Attack

Reddy et al.'s scheme has problem on A DoS attack. Their scheme use random number for preventing the replay attack but does not use timestamp so the scheme is weak on DoS. The attacker can obtain and intercept the previous authentication message $\{AID_U, N_U$ and $Y\}$ in the public communication. The attacker sends $\{AID_U, N_U$ and $Y\}$ again after authentication phase ends. But the server cannot found out that the message is previous message and cannot checks the legitimacy of incoming message because the server cannot check and know the freshness of message before $auth_U$ is same to $h(SK_S\|PID_U\|\beta)$. So the server executes various operation such as generating the random number operation, • operation, hash operation, and exclusive OR operations before checking whether the attacker's $auth_U$ and computed $h(SK_S\|PID_U\|\beta)$ are same. so the attacker can execute the DoS attack without difficulty.[7-9]

3-3 Wrong password change phase

Reddy et al.'s authentication scheme has procedural problem. If an user changes own password, first the user inputs ID_U and PW_U. So, the user's SC computes r_U , M and verifies V_2 as follows. $r_U=V_1\oplus h(ID_U\|PW_U)$, $V_2=\mathrm{h}(PID_U \|h(PW_U\|r_U))$, $M = N'\oplus h(PW_U \| r_U)$.

And the user chooses a new password PW_U^{new} and have to compute RPW^{new} as follows. $RPW^{new} = h(PW_U^{new} \| r_U) \oplus r$. But the user cannot compute RPW^{new} because the user does not know parameter r. parameter r does not store in the smart card and cannot compute r using other parameters. A parameter related r in smart card is only N' as follows.

$N' = N \oplus r$, $N = M \oplus RPW$

$N = h(PID_U \|ID_S \| k) \oplus h(PW_U \| r_U) \oplus r$

$\rightarrow N' = h(PID_U \|ID_S\|k)\oplus h(PW_U\|r_U \oplus r \oplus r$

$\rightarrow N' = h(PID_U\|ID_S \| k)\oplus h(PW_U \| r_U)$

N' does not contain the information about r because the parameter r is removed by $\oplus$ operation. So the user of Reddy et al.'s scheme cannot change the user's password because user cannot calculate parameter r.

3.4 Session key disclosure attack

An attacker can calculate the session key SK including previous session key using SK. Reddy et al.'s authentication scheme is weak on session key disclosure attack. An attacker can obtains all of AID, X including previous AID, X in public communication In this scheme, Using an power analysis, an attacker found out user's smart card, the attacker can extracts all information from the smart card. And he can compute user's ID_U and PW_U using the stored information. So he has AID, X, ID_U, PW_U, N', and V_1, so he can calculate the session key.

r_U = V_1 h (ID_U || PW_U),
PID_U = h (ID_U || r_U) [using computed r_U],
$N`_U$ = $AID_U \oplus PID_U$ [using computed PID_U],
M = N' ⊕ $h(PW_U \| r_U)$ [using computed r_U],
β = M X [using computed M],
N_S = β • $N`_U$ [using computed β]
→ SK_U = h (PID_U || $N`_S$ || β)

The attacker computes all formula's parameter of session key SK_U = h (PID_U || $N`_S$ || β). It is important that the attacker can computes all of session key including previous session key.

Ⅳ. Security enhanced authentication scheme

This section proposes an improved anonymous two-factor authentication with key-agreement for session initiation protocol using elliptic curve cryptography based various studies.[10-20]

4-1 System initialization phase

Before the protocol is ever executed, this scheme computes and shares the secret.

(1) S generates a point P on an elliptic curve $E(a, b)$ over F_p.

(2) S selects $h(\bullet)$ and Pri_S , and calculates $Pub_S = Pri_S \bullet P$.

(3) S stores Pri_S and publishes $\{E(a, b), P, Pub_S, h(\bullet)\}$.

4-2 User registration phase

For a user U, this phase is executed once when User U registers itself with the server.

(1) User U selects ID_U and two random numbers r_U and r. Then U imprints biometrics BIO_i and Generate R_i, P_i and PID_U, RPW.

$Gen(BIO_i') = < R_i , P_i >$,

$PID_U = h (ID_U \| r_U)$, $RPW = h (PW_U \| r_U) \oplus r$

And U sends registration request { ID_U , RPW } to S using a secure communication.

(2) S calculates M, N as follows;

$M = h (PID_U \| ID_S \| k)$, $N = M \oplus RPW$

And then, S inputs { N, P, Pub_S , $h(\bullet)$ } on user's smart card SC and send it to U .

(3) U computed V_1 , N', V_2, V_3 as follows.

$V_1 = r_U \oplus h(ID_U \| PW_U$,
$N' = N \oplus r = M \oplus h (PW_U \| r_U)$,
$V_2 = h(PID_U \| h(PW_U \| r_U))$,
V3 = $r \oplus h(ID_U \| R_i \| r_U))$

And then, U stores them on the received smart card SC. Therefore SC(Smart Card) stores { N , V_1 ,V_2 , V_3 , P, P_i , Pub_S , $h(\bullet)$}. Figure 3 shows user registration phase of proposed scheme.

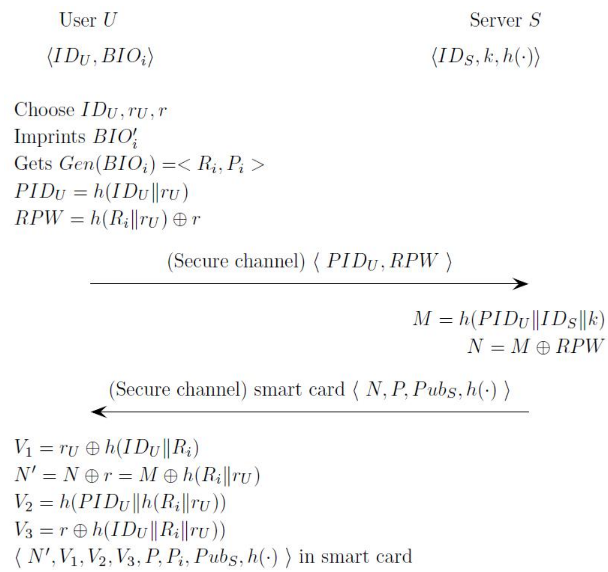

Fig. 3. User registration phase of proposed scheme

4-3 Key agreement authentication phase

This paper proposed secure authentication scheme with key-agreement phase, user U and server S can authenticate each other and the they compute a session-key of them. Figure 4 shows the process of authentication phase.

(1) U inserts SC and enters ID_U and imprint BIO_i. Then SC computes R_i, r_U, and PID_U .

$R_i = Rep(BIO'_i, P_i)$, $r_U = V_1 \oplus h (ID_U \| PW_U)$, $PID_U = h (ID_U \| r_U)$. And checks the accuracy of V_2 . $V_2 = h (PID_U \| h (PW_U \| r_U))$. And then the SC generates a random number a and computes N_U, AID_U, timestamp T_1, M , Y as follows;

$N_U = a \bullet P$, $N`_U = a \bullet Pub_S$ , $AID_U = PID_U \oplus N`_U$, $M = N' \oplus h (PW_U \| r_U)$, $Y = h (PID_U \| N_U \| M \| T_1)$. User U sends the REQUEST(AID_U, N_U, Y, T_1) to server S.

(2) S checks the received timestamp T_1, and calculates $N`_U$ , $PID_U$, $M$. $N`_U = Pri_S \bullet N_U$, $PID_U = AID_U \oplus N`_U$, $M = h(PID_U \| ID_S \| k)$.

And then, verifies $Y = h (PID_U \| N_U \| M \| T_1)$. If they are not same, process aborts. S generates a random number β and computes X, N_S, SK_S, $auth_S$, S's timestamp T_2. $X = M \oplus \beta$, $N_S = \beta \bullet N`_U$, $SK_S = h(PID_U \| N_S \| \beta)$, *Generate* T_2, $auth_S = h (SK_S \| PID_U \| M \| T_2)$.

S sends $CHALLENGE(realm, X, auth_S, T_2)$ to U.

(3) U receives $CHALLENGE$ messages, SC checks timestamps T_2 and computes β, $N`_S$, SK_U.

$\beta = M \oplus X$, $N`_S = \beta \cdot N`_U$, $SK_U = h(PID_U \| N`_S \| \beta)$

And then checks $auth_S$ messages as follows;

$auth_S = h(SK_U \| PID_U \| M \| T_2)$

If $auth_S$ is same to $h(SK_U \| PID_U \| M \| T_2)$, U generates T_3 and computes $auth_U$. $auth_U = h(SK_U \| PID_U \| \beta \| T_3)$. And then, U sends the $RESPONSE(realm, auth_U)$ to server S.

(4) S checks T_3 and $auth_U = h(SK_S \| PID_U \| \beta)$. If they are same, S computed session key $SK_U = SK_S$ for using next communication.

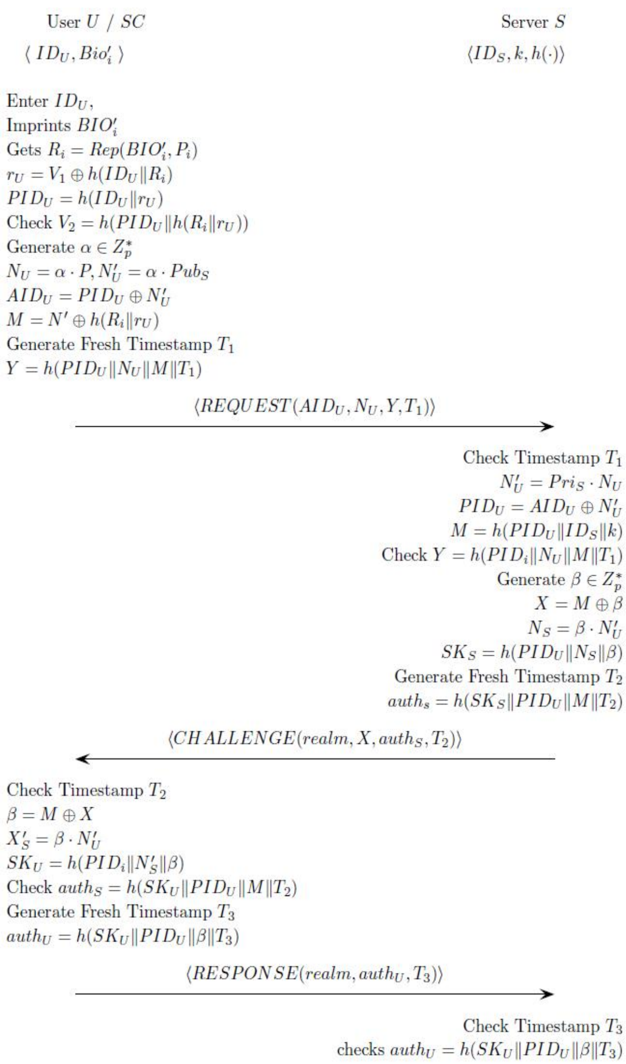

Fig. 4. Key agreement authentication phase of proposed scheme

4-4 Biometrics updating phase

Proposed scheme allows users to freely update biometrics on biometrics updating phase as shown in Figure 5.

User U

$\langle ID_U, BIO_i \rangle$

Input ID_U,

Imprints BIO'_i

Gets $R_i = Rep(BIO'_i, P_i)$

$r_U = V_1 \oplus h(ID_U \| R_i)$

$r = V_3 \oplus h(ID_U \| R_i \| r_U))$

Checks $V_2 = h(PID_U \| h(R_i \| r_U))$

Imprints BIO''_i

Gets $Gen(BIO''_i) = < R_{inew}, P_{inew} >$

$M = N' \oplus h(R_{inew} \| R_U)$

Computes $RPW^{new} = h(R_{inew} \| r_U) \oplus r$

$V_{1new} = r_U \oplus h(ID_U \| R_{inew})$

$N'_{new} = N \oplus r = M \oplus h(R_{inew} \| r_U)$

$V_{2new} = h(PID_U \| h(h(R_{inew} \| r_U))$

$V_{3new} = r \oplus h(ID_U \| R_{inew} \| r_U))$

$\langle N'_{new}, V_{1new}, V_{2new}, V_{3new}, P, P_{inew}, Pub_S, h(\cdot) \rangle$ in smart card

Fig. 5. Biometrics updating phase of proposed scheme

(1) U inserts SC and enters the own user's ID_U and imprint BIO'_i. SC computes R_i, r_U, r as follows ; $R_i = Rep(BIO'_i, P_i)$, $r_U = V_1 \oplus h(ID_U \| R_i)$, $r = V_3 \oplus h(ID_U \| R_i \| r_U))$. And then, SC verifies the computed value and V_2 as follows; $V_2 = h(PID_U \| h(R_i \| r_U))$. If $V_2 = h(PID_U \| h(R_i \| r_U))$ are same, then U imprint new BIO_i , generate new R_{inew} and P_{inew} and compute $M = N' \oplus h(R_{inew} \| r_U)$.

(2) U computes RPW^{new}, V_{1new}, V_{2new}, V_{3new}, , N'_{new} as follows; $RPW^{new} = h(R_{inew} \| r_U) \oplus r$,

$V_{1new} = r_U \oplus h(ID_U \| R_{inew})$,

$N'_{new} = M \oplus h(R_{inew} \| r_U)$,

$V_{2new} = h(PID_U \| h(R_{inew} \| r_U))$,

$V_{3new} = r \oplus h(ID_U \| R_{inew} \| r_U))$.

And then, user U replaces the existing values on the smart card as follows.

$\{N'_{new}, V_{1new}, V_{2new}, P, P_{inew}, Pub_S, h(\cdot)\}$.

Ⅴ. Security analysis of Proposed scheme

This paper compares the security analysis on Lu et al., Reddy et al., and the proposed scheme. Table 2 shows the security analysis comparison as follows.

Reddy et al. execute security analysis and a proposed the enhanced anonymous two-factor mutual authentication with key-agreement scheme for session initiation protocol. Lu et al.'s scheme is secure DoS attack and provide secure password change phase. But Reddy et al. ’s scheme is provide ①, ②, ③, ④ but have important security problems on ⑤, ⑥, ⑦, ⑧ as mentioned this paper. The proposed scheme is secure and providing the user anonymity, mutual authentication, protect sensitive information, impersonation attack, off-line password guessing attack, DoS attack, secure password change phase, session key disclosure attack using the biometrics BIO_i, V_3 and timestamp T. And proposed scheme changes the values of Y, $auth_U$, $auth_S$ due to protecting DoS attack. The biometrics using fuzzy extraction BIO_i, R_i, P_i provides the security probability on off-line password guessing attack, session key disclosure attack.

Table 2. Security analysis comparison

Security analysis	Lu et al.	Reddy et al.	Proposed
① User anonymity	No	Yes	Yes
② Mutual authentication	No	Yes	Yes
③ Protect sensitive information	No	Yes	Yes
④ Impersonation attack	weak	secure	secure
⑤ Off-line password guessing attack	weak	weak	secure
⑥ DoS attack	secure	weak	secure
⑦ Secure password change phase	Yes	No	Yes (BIO)
⑧ Session key disclosure attack	weak	weak	secure

Ⅵ. Conclusion.

This paper discussed possible attacks for Reddy et al.'s authentication scheme, and a modified scheme was proposed to improve security and protect against various attacks such as off-line password guessing attack, DoS attack, secure password change phase, session key disclosure attack. This scheme was security enhanced anonymous two factor mutual authentication scheme with key agreement more than other scheme.

Acknowledge

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

References

[1]Johnston, Alan. "SIP: understanding the session initiation protocol, Artech House." Inc., Norwood, 2003

[2]Rosenberg, Jonathan, et al. SIP: session initiation protocol. No. RFC 3261. 2002.

[3]Lu, Yanrong, et al. "An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography." *Multimedia Tools and Applications* 76.2, 1801-1815, 2007.

[4]Reddy, Alavalapati Goutham, et al. "An enhanced anonymous two-factor mutual authentication with key-agreement scheme for session initiation protocol." Proceedings of the 9th International Conference on Security of Information and Networks. ACM, 2016.

[5]He, Debiao, Jianhua Chen, and Yitao Chen. "A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography." *Security and Communication Networks,* 1423-1429, 2012.

[6]Ma, Chun-Guang, Ding Wang, and Sen-Dong Zhao. "Security flaws in two improved remote user authentication schemes using smart cards." *International Journal of Communication Systems* 27.10, 2014

[7]Choi, Younsung, et al. "Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics." The Scientific World Journal 2014.

[8]Choi, Younsung. "Cryptanalysis on Anonymous Two Factor Mutual Authentication with Key Agreement Scheme For Session Initiation Protocol." *Research Journal of Applied Sciences* 12.5, 2017

[9]He, Debiao, and Sherali Zeadally. "An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography." IEEE internet of things journal 2.1, 2015.

[10]Chaudhry, Shehzad Ashraf, et al. "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography." Electronic Commerce Research 16.1: 113-139, 2016.

[11]Chaudhry, Shehzad Ashraf, "An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography." *Journal of Medical Systems* 39.11, 2015.

[12]Reddy, Alavalapati Goutham, et al. "A secure anonymous authentication protocol for mobile services on elliptic curve cryptography." IEEE Access 4, 2016.

[13]Choi, Younsung, et al. "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography." *Sensors* 14.6, 2014

[14]Farash, Mohammad Sabzinejad, Saru Kumari, and Majid Bakhtiari. "Cryptanalysis and improvement of a robust smart card secured authentication scheme on SIP using elliptic curve cryptography." *Multimedia Tools and Applications* 75.8, 4485-4504, 2016.

[15]Choi, Younsung, Youngsook Lee, and Dongho Won. "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction." *International Journal of Distributed Sensor Networks* 12.1, 2016.

[16]Madhusudhan, R., and R. C. Mittal. "An efficient fingerprint-based remote user authentication protocol using mobile devices." *Proceedings of the International Conference on Soft Computing for Problem Solving* (SocProS 2011) December 20-22, 2011. Springer, India, 2012.

[17]Kumari, Saru, Muhammad Khurram Khan, and Rahul Kumar. "Cryptanalysis and improvement of 'a privacy enhanced scheme for telecare medical information systems'." *Journal of medical systems* 37.4 , 2013.

[18]Li, Xiong, et al. "Robust dynamic ID-based remote user authentication scheme using smart cards." *International journal of ad hoc and ubiquitous computing* 17.4, 2014.

[19]H. J. Yang, D. H. Kim, and Y. G. Seo, "Noise-robust Hand R egion Segmentation In RGB Color-based Real-time Image", *The Journal of Digital Contents Society*, 18(8), p1603-1613, Dec, 2017.

[20]K. H. Park and H. S. Noh, "Effective Acne Detection using Component Image a* of CIE L*a*b* Color Space," *Journal of Digital Contents Society*, Vol. 19, No. 7, pp. 1397-1403, July 2018.

Younsung Choi

2006.2 : Sungkyunkwan University, Information and Communication Engineering (B.S Degree

2007.8 : Sungkyunkwan University, Department of Electrical and Computer Engineering(M.S Degree)

2015.8 : Sungkyunkwan University, Department of Electrical and Computer Engineering(Ph.D Degree)

2010.6～2013.5 : Department of Information engineering, Korea Army Academy at Yeong-Cheon, Assistant professor

2016.3～now: Major of Cyber Security, Division of Computer, Howon University, Assistant professor

※Research Interests : Information security, Digital forensics, Cloud security