Journal of Korea Multimedia Society Vol. 19, No. 3, March 2016(pp. 585-594)
http://dx.doi.org/10.9717/kmms.2016.19.3.585

순방향 안전성을 제공하는 대칭키 기반의 원격 사용자 인증 방식

이성엽[†], 박기성[††], 박요한[†††], 박영호[††††]

Symmetric Key-Based Remote User Authentication Scheme With Forward Secrecy

SungYup Lee[†], KiSung Park[††], YoHan Park[†††], YoungHo Park[††††]

ABSTRACT

Recently because of development of remote network technology, users are able to access the network freely without constraints of time and space. As users are getting more frequent to access the remote server in a computing environment, they are increasingly being exposed to various risk factors such as forward secrecy and server impersonation attack. Therefore, researches for remote user authentication scheme have been studying actively. This paper overcomes the weaknesses of many authentication schemes proposed recently. This paper suggests an improved authentication scheme that protects user's anonymity with preserving variable more safe and also provides forward secrecy.

Key words: Remote User Authentication Scheme, Symmetric Key, Forward Secrecy, Smart Card

1. 서 론

최근 네트워크 기술의 급속한 발전으로 사용자는 시간이나 장소에 구애받지 않고 인터넷 서비스를 이용할 수 있게 되었다. 원격 사용자 인증 방식은 원격 서비스나 자원을 보호하기 위해서 비인가 사용자에 의한 접근을 통제하며 정당한 사용자를 검증하는 매우 중요한 과정이다. 하지만 원격 환경에서의 인증 방식은 비밀키가 노출되더라도 키 분배 과정에서 생성된 세션키의 안전성을 지원하는 순방향 안전성을 제공하기 어려우며 사전, 위장, 추측 공격과 같은 보안의 취약점들이 존재한다. 따라서 원격 서버와 원격 사용자 사이의 안전한 인증을 위하여 기밀성, 무결성 및 가용성이 제공되어야하며 순방향 안전성을 제공하는 안전한 원격 사용자 인증 방식이 필요하다[1-4].

최근 연구된 원격시스템 환경에서 사용자 인증의 대표적 방식들은 다음과 같다. 2011년 Khan 등은[5] Wang 등이[6] 제안한 방식에서 공격자가 로그인 메시지를 획득하면 사용자의 익명성을 보장할 수 없고 서버가 사용자에게 임의의 비밀번호를 부여하여 내부자 공격에 취약하다고 주장하였으며 이러한 약점을 극복한 dynamic ID기반의 원격 사용자 인증 방식을 제안하였다. 2012년 Chen 등은[7] Khan 등이 제안한 dynamic ID기반의 원격 사용자 인증 방식에서

※ Corresponding Author : YoungHo Park, Address: (702-701) 80 Daehakro, Bukgu, Daegu, Korea, TEL : +82-53-950-7842, FAX : +82-53-950-5505, E-mail : parkyh@knu.ac.kr
Receipt date : Nov. 12, 2015, Revision date : Jan. 5, 2016
Approval date : Jan. 12, 2016
[†] School of Electronics Engineering, Graduate School, Kyungpook National University
(E-mail : lsy0307@ee.knu.ac.kr)
[††] School of Electronics Engineering, Graduate School, Kyungpook National University
(E-mail : kisung2@ee.knu.ac.kr)
[†††] School of Electronics Engineering, Kyungpook National University
((E-mail : hanny12@gmail.com)
[††††] School of Electronics Engineering, Kyungpook National University

내부자 공격에 취약하고 등록하지 않는 변수를 사용하는 문제가 있다고 주장하였으며 변수 사용 문제를 개선하고 사용자의 랜덤 값을 공개 채널로 보내지 않는 인증 방식을 제안하였다. 2013년 Jiang 등은[8] Chen 등의 방식이 사용자의 익명성과 불추적성이 제공되지 않아 추측 및 tracking 공격에 취약하다고 주장하였고 사용자의 익명성과 불추적성이 제공되는 대칭키 방식의 향상된 인증 방식을 제안하였다. 2013년 Kumari 등은[9] Jiang 등의 방식이 사용자 가장, 추측 그리고 DoS(denial of service) 공격에 취약하다고 주장하였으며 이러한 문제점들을 보완하여 TMIS(telecare medical information system)에 적합한 방식을 제안하였다. 그러나 Kim 등은[10] Kumari 등의 방식이 순방향 안전성과 사용자의 익명성을 보장하지 못하는 문제점을 발견하고 공격자가 비밀키를 알면 ID와 서버의 랜덤 변수를 획득하여 세션키를 찾아낼 수 있다고 주장하였다. 따라서 순방향 안전성을 제공하며 사용자의 익명성을 보장하는 인증 방식이 요구된다.

본 논문은 원격 환경에서 사용자의 익명성을 보호하며 순방향 안전성을 제공하는 인증 방식을 제안한다. 제안하는 방식에는 Kumari 등의 방식보다 변수를 안전하게 보호하고 대칭키를 사용하여 ID를 암호화/복호화한다. 또한 사용자는 ID를 새로운 변수와 XOR연산하여 서버에 전송하므로 사용자의 익명성을 보호한다. 따라서 공격자가 비밀키를 획득해도 세션키를 찾을 수 없으므로 순방향 안전성을 제공한다. 제안한 방식은 Kumari 등의 등록 단계에서 패스워드를 랜덤 값과 연산을하여 서버는 사용자의 패스워드를 알 수 없는 장점은 그대로 유지하면서 순방향 안전성 및 스마트카트 lost 공격에 대한 문제점을 개선한 인증 방식이다.

2. 기존의 사용자 인증 방식

정보를 보호하고 안전한 로그인 요청을 생성하기 위해서 원격 기반 인증 방식들이 활발히 연구되고 있다. 본 장에서는 원격 기반 인증 방식의 대표적인 방식인 Khan 등의[5] 원격 사용자 인증 방식, Chen 등의[7] 인증 방식, Jiang 등의[8] 인증 방식 그리고 Kumari 등의[9] 인증 방식에 관하여 분석한다. 각각의 인증 방식은 등록 단계, 로그인 단계 및 인증 단계의 세 단계로 구성된다.

2.1 Khan 등의 인증 방식

Khan 등은[5] Wang 등이[6] 제안한 방식에서 인증 단계 중 사용자의 익명성을 보호받지 못하는 취약점을 파악하고, 공격자가 로그인 메시지를 획득하면 ID를 얻을 수 있다는 것을 보였다. 또한 Wang 등이 제안한 timestamp를 사용하여 재사용 공격에 안전한 이점은 그대로 유지하며 기존의 방식보다 향상된 dynamic ID기반의 인증 방식을 제안하였다.

Khan 등의 방식은 아래의 Fig. 1, 2, 3과 같이 등록, 로그인 그리고 인증 단계로 이루어진다. Khan 등은 기존의 Wang 등의 서버가 패스워드를 임의로 생성

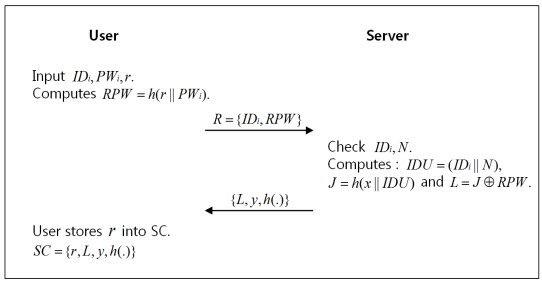

Fig. 1. Registration phase of the scheme of Khan et al..

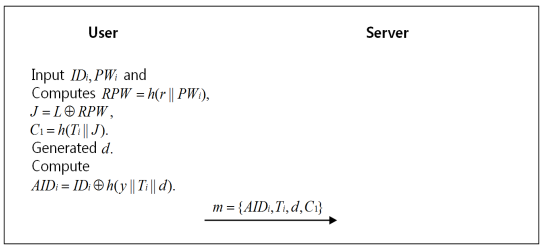

Fig. 2. Login phase of the scheme of Khan et al.

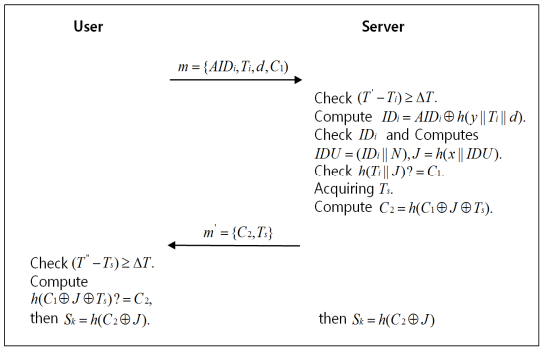

Fig. 3. Authentication phase of the scheme of Khan et al.

하여 사용자에게 전송하고 ID를 서버에 평문으로 전송하는 문제점을 개선하기 위해 dynamic ID기반의 인증 방식을 제안하였다. 등록 단계에서 서버는 사용자의 동의 없이 패스워드를 만들지 않고 사용자가 패스워드를 만들어 패스워드와 random nonce r을 이용하여 $RPW = h(r \| PW_i)$를 만들어 서버에게 전송한다. 로그인 단계에서 dynamic ID를 성취하기 위하여 사용자는 등록 단계에서 생성한 $IDU = (ID_i \| N)$를 이용해 $AID_i = ID_i \oplus h(y \| T_i \| d)$를 만들고 인증 단계에서 서버는 IDU와 AID를 체크하여 ID를 인증하는 방식이다. 따라서 Khan 등은 Wang 등의 인증 방식의 문제점을 개선한다고 주장하였다.

2.2 Chen 등의 인증 방식

Chen 등은[7] Khan 등이 제안한 인증 방식에서 내부자 공격에 여전히 취약하다는 점을 발견하였다. Chen 등은 인증 단계에서 사용되는 파라미터의 일부 값들이 모든 내부자에게 공유가 된다는 점을 발견하고, ID값을 획득하여 위장공격이 가능함을 보였다. Khan 등의 인증 방식에는 스마트카드 안에 중요한 정보가 저장되어 있다. 만약 공격자가 스마트카드를 획득하면 Khan 등이 제안한 익명성과 안전성은 보장될 수 없다. 이러한 이유로 Chen 등은 아래의 Fig. 4, 5, 6과 같이 등록, 로그인 그리고 인증 단계로 제안하였다.

Chen 등은 기존의 Khan 등의 인증 방식이 여전히 내부자 공격에 취약하고 스마트카드의 정보로 ID를 찾을 수 있는 문제점을 개선하기 위해 dynamic ID 기반의 향상된 인증 방식을 제안하였다. 등록 단계에서 서버는 사용자의 ID 및 변수 N값을 RGR(registration record)에 저장하고 $y_u = h(RPW_u \| ID_u)$ 변수를

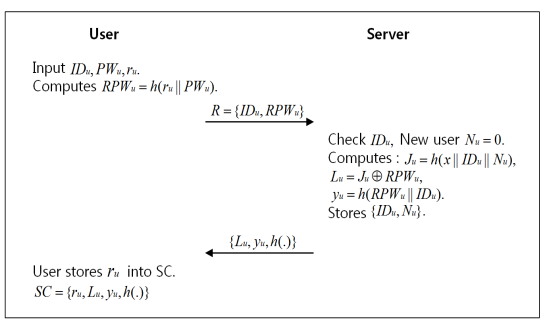

Fig. 4. Registration phase of the scheme of Chen et al.

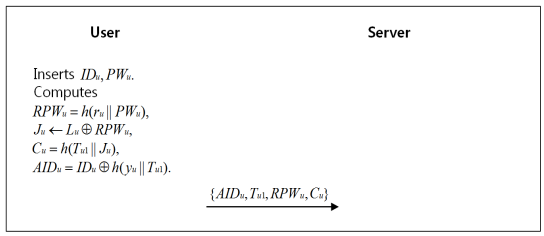

Fig. 5. Login phase of the scheme of Chen et al.

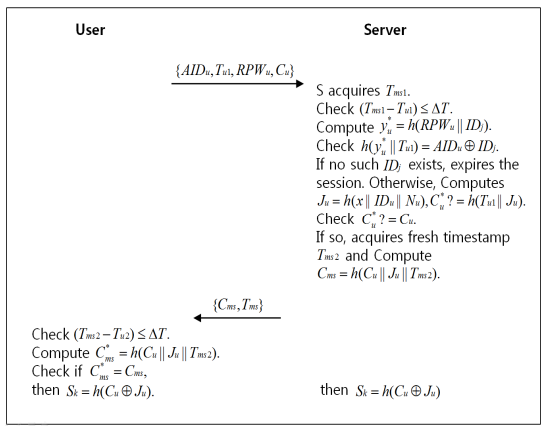

Fig. 6. Authentication phase of the scheme of Chen et al.

생성하였다. 로그인 단계에서 Khan 등은 변수 J를 생성하지만 Chen 등은 등록 단계에서 생성한 $L_u = J_u \oplus RPW_u$를 이용하여 J_u를 찾아내는 방법을 사용하였다. 변수 J_u를 이용하여 $C_u = h(T_u 1 \| J_u)$를 만들고 인증 단계에서 $C_u^* = C_u$를 체크하여 상호인증을 제공하였다. 따라서 Chen 등이 제안한 방식은 익명성을 보장하고 내부자 공격에 안전하다고 주장하였다.

2.3 Jiang 등의 인증 방식

Jiang 등은[8] Chen 등이 제안한 인증 방식에서 사용자의 익명성과 불추적성이 제공되지 않고 ID 추측 및 tracking 공격이 가능하다고 주장하였다. Jiang 등은 Chen 등의 방식이 스마트카드의 정보와 로그인 요청 메시지를 획득하면 취약하다고 주장하였다. 이러한 이유로 Jiang 등은 사용자의 익명성과 불추적성이 제공되는 향상된 인증 방식을 제안하였다. 아래의 Fig. 7, 8, 9는 Jiang 등이 제안한 등록, 로그인 그리고 인증 단계이다.

Jiang 등은 Chen 등의 방식과 다르게 등록 단계에

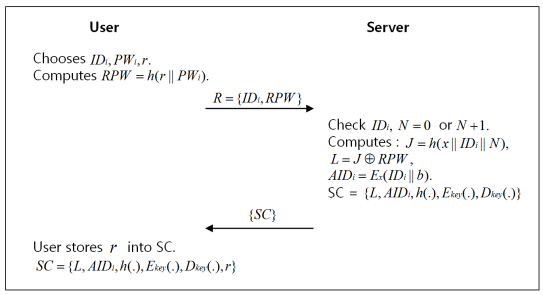

Fig. 7. Registration phase of the scheme of Jiang et al.

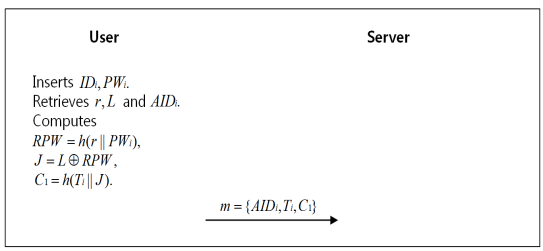

Fig. 8. Login phase of the scheme of Jiang et al.

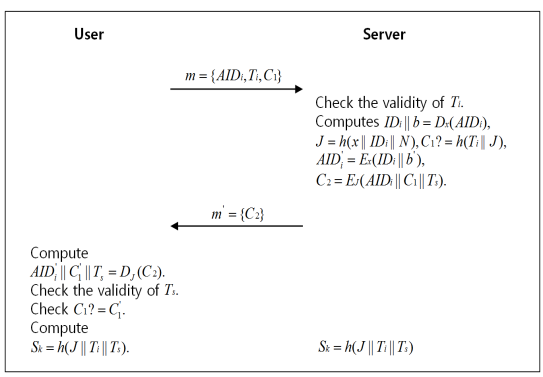

Fig. 9. Authentication phase of the scheme of Jiang et al.

서 대칭키를 사용하여 $AID_i = E_x(ID_i \| b)$를 만들었다. 또한 로그인 단계에서 사용자는 random nonce r, 변수 L 그리고 AID_i를 ID_i 및 PW_i를 이용하여 찾아오고 인증 단계에서 서버는 $AID_i = E_x(ID_i \| b)$를 복호화하여 ID_i를 찾아내는 방식이다. 그래서 공격자가 비밀키 및 변수 J값을 획득하지 못하면 익명성을 보장한다고 주장하였다. 또한 사용자의 불추적성을 제공하기 위해 암호화/복호화를 사용하여 성취하였다. Chen 등의 방식 역시 스마트카드 안에 중요한 정보가 저장되어 있다. 만약 공격자가 스마트카드의 정보를 획득하면 ID 및 패스워드를 공격자가 획득할 수 있다. 하지만 Jiang 등은 대칭키 방식을 사용하여 Chen 등의 방식을 개선했다고 주장하였다.

2.4 Kumari 등의 인증 방식

Kumari 등은[9] Jiang 등의 방식이 스마트카드를 분실하거나 도난당할 경우, 스마트카드 안에 저장되어 있는 random nonce r에 의해 비밀번호 추측 및 사용자 위장 공격이 가능함을 보였다. 또한 Jiang 등의 방식은 등록 단계에서 RGR(registration record)에 ID를 평문으로 저장해 Privileged 내부자 공격이 가능함을 보였다. Kumari 등은 Jiang 등의 문제점을 개선하여 아래의 Fig. 10, 11, 12와 같이 등록, 로그인 그리고 인증 단계로 제안하였다.

Kumari 등의 방식은 Jiang 등의 방식과 달리 등록 단계에서 변수 $M = h(J \| RPW \| ID)$ 및 $K = h(ID \| PW) \oplus r$를 만들었다. 그래서 로그인 단계에서 사용자는 변수 K를 이용하여 random nonce r을 찾아오고 $RPW^* = h(r^* \| PW)$를 생성하였다. 또한 RPW를 이용하여 변수J 값을 찾아오고 $M^* = h(J^* \| RPW^* \| ID)$을 생성하였다. 생성된 변수 M^*은 인증 단계에서 서버가 상

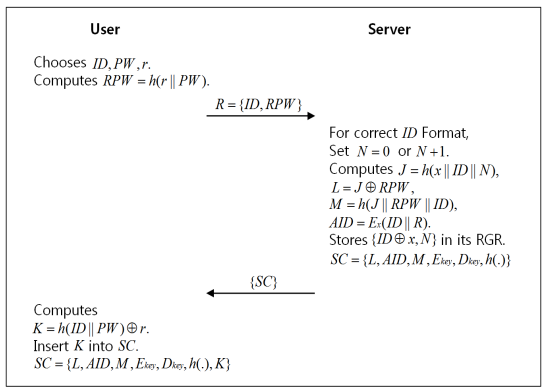

Fig. 10. Registration phase of the scheme of Kumari et al.

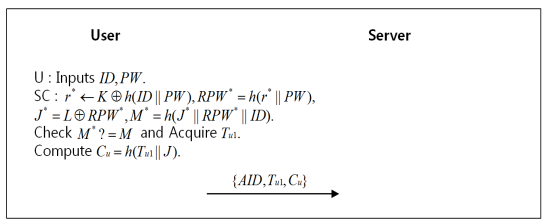

Fig. 11. Login phase of the scheme of Kumari et al.

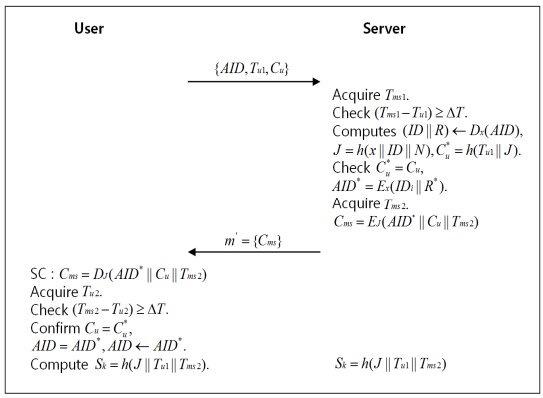

Fig. 12. Authentication phase of the scheme of Kumari et al.

호인증을 성취하기위해 사용하였다. 따라서 Kumari의 방식은 random nonoce r을 스마트카드에 평문으로 저장하지 않고 ID는 RGR에 평문으로 저장하지 않으므로 중간자 공격 및 비밀번호 추측공격에 안전하다고 주장하였다.

3. 제안한 원격 사용자 인증 방식

본 논문에서는 Kumari 등의[9] 방식이 가진 장점을 그대로 보존하면서 순방향 비밀유지 및 스마트카드 분실 공격에 안전한 방식을 제안하였다. Kumari 등의 방식은 순방향 비밀유지에서 공격자가 비밀키를 안다고 가정하면 세션키를 얻을 수 있는 방식이다. 공격자가 $AID = E_x(ID \| R)$를 복호화하면 사용자의 ID와 서버의 랜덤 값 R을 획득하게 된다. 획득한 ID를 이용하여 변수 J를 찾게 되면 쉽게 이전의 세션키를 찾을 수 있다. 하지만 제안한 방식에는 $AID = E_x(ID \oplus h(Y \| b))$를 사용하여 비밀키를 획득해도 Y값과 b값을 모르기 때문에 ID를 획득할 수가 없다. 또한 변수 J값은 변수 R, A 그리고 L값으로 되찾아오는 방식이다. 따라서 공격자가 스마트카드의 정보를 획득해도 스마트카드 분실 공격에는 안전한 방식이다. Table 1은 본 논문에서 사용되는 변수 및 표기법을 기술한 것이다.

위 Fig. 13은 제안한 방식 중 등록 단계를 나타내고 등록 단계는 아래와 같은 과정으로 이루어진다.

1) 사용자는 ID와 PW를 선택하고 random nonce r을 생성한다.

Table 1. Notations

Notations	Meanings
U_i	A user
S_i	A remote medical server
ID	The identity of U_i
PW	The password of U_i
RGR	A registration record
N	The number of times U_i registers with the server
r	A random nonce of U_i
T_x	A timestamp
x	The S_i's secret key
b	The S_i's random number
$\|$	The concatenation operator
$\oplus$	The Exclusive-OR operator
$h(.)$	The secure one-way hash function
$E_k(.)/D_k(.)$	A symmetric cryptographic encryption/decryption using a key k

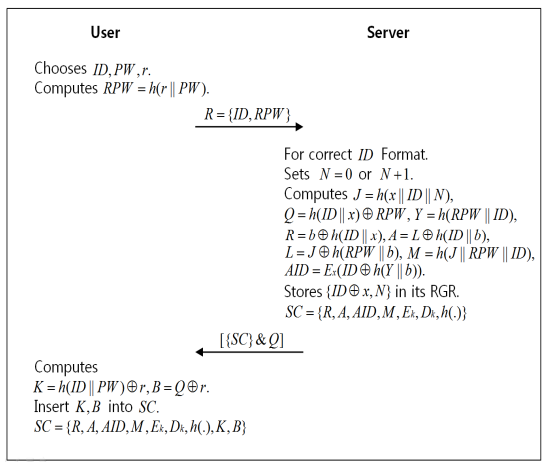

Fig. 13. Registration phase of the proposed scheme.

2) PW와 r을 이용하여 $RPW = h(r \| PW)$를 만들고 ID와 RPW를 secure channel로 서버에 전송한다.

3) ID와 RPW를 받은 서버는 먼저 ID 형태가 올바른지 체크를 하고, 등록된 시간의 넘버를 부여한다. 신규 사용자이면 N = 0이고 재등록 사용자이면 N + 1 부여한다.

4) 서버는 $J = h(x \| ID \| N)$, $Q = h(ID \| x) \oplus RPW$, $Y = h(RPW \| ID)$, $R = b \oplus h(ID \| x)$, $A = L \oplus h(ID \| b)$, $L = J \oplus h(RPW \| b)$, $M = h(J \| RPW \| ID)$, $AID = E_x(ID \oplus h(Y \| b))$를 계산하고 RGR에 $\{ID \oplus x, N\}$을 저장한다.

5) 서버는 스마트카드에 $\{R, A, AID, M, E_k, D_k, h(.)\}$을 저장하고 스마트카드와 변수 Q를 사용자에게 secure channel로 보낸다.

6) 사용자는 스마트카드와 Q를 받고 $K = h(ID \| PW) \oplus r$, $B = Q \oplus r$을 계산하고 스마트카드 안에 저장한다.

위 Fig. 14은 제안한 방식 중 로그인 & 인증 단계를 나타내고 로그인 & 인증 단계는 아래와 같은 과정으로 이루어진다.

1) 사용자는 인증을 위해 스마트카드를 기기에 넣고 ID와 PW를 입력한다.

2) 입력받은 ID와 PW를 이용하여 스마트카드는 $r^* \leftarrow K \oplus h(ID \| PW)$을 찾아오고 $RPW^* = h(r^* \| PW)$를 계산한다.

3) RPW를 이용하여 스마트카드는 $h(ID \| x)^* \leftarrow B \oplus RPW^* \oplus r^*, b^* \leftarrow h(ID \| x)^* \oplus R$, $L^* \leftarrow A \oplus h(ID \| b^*)$, $J^* \leftarrow L^* \oplus h(RPW^* \| b^*)$, $M^* = h(J^* \| RPW^* \| ID)$를 계산한다.

4) 스마트카드는 $M^* = M$ 같은지 체크하고 같으면 $C_u = h(T_{u1} \| J)$를 계산한다. 만약 값이 다르면 세션을 종료한다.

5) 사용자는 로그인 메시지 = $\{AID, T_{u1}, RPW, C_u\}$를 public channel로 서버에게 전송한다.

6) 서버가 로그인 메시지를 받고 T_{ms1}을 생성한다. 그리고 $(T_{ms1} - T_{u1}) > \Delta T$를 체크한다. 만약 조건이 맞지 않다면 세션을 종료한다.

7) 로그인 메시지의 RPW를 이용하여 서버는 $Y^* = h(RPW \| ID^*)$를 생성하고 $ID^* \oplus h(Y^* \| b) ?= D_x(AID)$를 체크한다. 만약 ID가 RGR에 존재하지 않으면 세션을 종료한다. ID^*값이 같으면 $J = h(x \| ID \| N)$, $C_u^* = h(T_{u1} \| J)$를 계산한다.

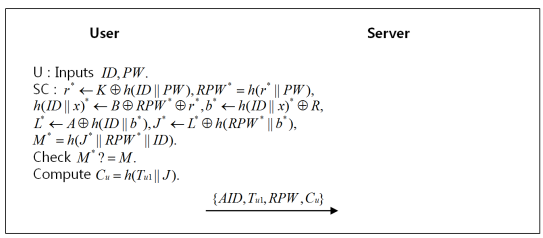

Fig. 14. Login phase of the proposed scheme.

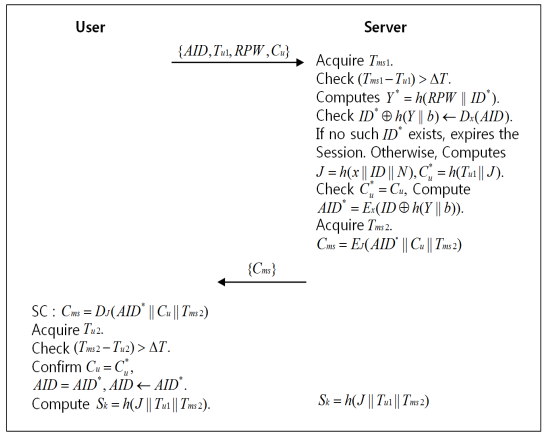

Fig. 15. Authentication phase of the proposed scheme.

8) $C_u^* = C_u$ 체크한다. 만약 같지 않으면 세션을 종료한다. 같으면 $AID^* = E_x(ID \oplus h(Y \| b))$를 계산하고 T_{ms2}를 생성한다.

9) 생성한 T_{ms2}를 이용하여 $C_{ms} = E_J(AID^* \| C_u \| T_{ms2})$를 계산하여 사용자에게 public channel로 보낸다.

10) 사용자는 C_{ms}를 받고 $C_{ms} = D_J(AID^* \| C_u \| T_{ms2})$를 계산하고 T_{u2}를 생성한다.

11) 생성한 T_{u2}를 이용하여 $(T_{ms2} - T_{u2}) > \Delta T$를 체크하고 조건에 만족하면 $C_u^* = C_u$ 같은지 확인한다. 만약 다르게 되면 세션을 종료한다.

12) $C_u^* = C_u$가 같다면 $AID^* = AID$ 같은지 확인을 하고 다르면 $AID \leftarrow AID^*$ 재배치한다.

13) 사용자와 서버는 세션키 $S_k = h(J \| T_{u1} \| T_{ms2})$를 생성하고 로그인 & 인증 단계를 마친다.

4. 분 석

Kumari 등의 인증 방식은 공격자에게 변수를 드러나지 않게 하기 위해 XOR연산을 이용하거나 새로운 변수를 만들어 전송하는 장점은 있지만 순방향 비밀유지와 스마트카드 분실 공격에 취약하다. 제안된 인증 방식은 Kumari 등의 인증 방식과 다르게 ID와 관련된 변수 값을 찾는 것이 어렵고 ID를 암호화/복호화하는 과정에서 랜덤 값과 변수를 XOR연산하여 공격자가 비밀키를 획득하더라도 ID를 찾을 수

없다. 본 논문에서 제안된 방식은 다음과 같은 informal analysis를 이용하여 안전성을 분석한다.

4.1 Lack of forward secrecy

순방향 비밀유지는 x를 공격자가 알아도 세션키는 안전해야한다. Kumari 등의 방식에서는 공격자가 AID를 복호화해서 ID를 찾으면 이전의 세션키를 획득할 수 있지만 제안한 방식에서는 $AID = E_x(ID \oplus h(Y\|b))$를 XOR연산 및 변수 Y의 값을 사용하여 공격자가 ID를 찾을 수 없도록 제안한다. 공격자가 ID를 찾기 위해서 변수 Y값 및 random number b를 얻어야 하는데, 공격자는 Y값 및 b값을 가지고 있지 않아 ID도 획득할 수 없고 세션키도 알 수 없다. 이러한 이유로 제안된 방식은 순방향 비밀유지를 제공하였다.

4.2 Lost smart card attack

제안한 방식은 공격자가 스마트카드를 습득해도 공격할 수 없다. 만약 공격자가 스마트카드를 습득하여 스마트카드에 저장되어 있는 값 $\{R, A, AID, M, E_k, D_k, h(.), K, B\}$을 얻었다고 해도 공격자는 ID, PW에 관한 어떠한 값도 알 수 없으므로 스마트카드 분실 공격에 대해 안전하다. Kumari 등의 방식에는 공격자가 $M = h(J\|RPW\|ID) \rightarrow h(L \oplus h(K \oplus h(ID\|PW)\|PW)\| h(K \oplus h(ID\|PW)\|PW)\|ID)$의 식으로 변경하여 후보 ID와 PW를 선택하여 $M^* = M$을 계산해 찾아냈지만, 제안된 방식에는 L값과 J값은 저장되어 있지 않고 R값, A값과 Q값에 의해 되찾아오는 방식이다. 따라서 공격자는 ID, PW를 찾을 수 없다. 이러한 이유로 제안된 방식은 스마트카드 분실 공격에 안전하다.

4.3 Online password guessing attack

제안된 프로토콜 안에 random nonce r은 사용자 스마트카드 안에 평문으로 저장되어 있지 않고 $K = h(ID\|PW) \oplus r$ 로 저장이 되어 있다. 따라서 공격자가 사용자의 스마트카드에 접근해도 ID와 PW를 알 수 없다. 또한 r을 얻기 위해서 공격자는 $K = h(ID\|PW) \oplus r$의 식을 이용해야 하는데 사용자의 ID와 PW를 알지 못하여 K의 식을 사용할 수 없고 r의 값을 알 수 없다. 이러한 이유로 제안된 방식은 온라인 패스워드 추측 공격에 안전하다.

4.4 Offline password guessing attack

공격자가 사용자의 스마트카드를 훔치거나 획득했다고 가정한다. 그래서 공격자는 스마트카드로부터 $\{R, A, AID, M, E_k, D_k, h(.), K, B\}$ 값을 획득할 수 있다. 사용자의 PW는 $Y = h(RPW\|ID)$, $B = Q \oplus r$, $Q = h(ID\|x) \oplus RPW$, $L = J \oplus h(RPW\|b)$, $K = h(ID\|PW) \oplus r$, $M = h(J\|RPW\|ID)$ 안에 들어있다. 공격자가 PW를 획득하려면, 공유된 secret J 와 random nonce r을 알아야한다. 하지만 J값과 L값은 사용자의 스마트카드나 서버에 평문으로 저장되어 있지 않다. 또한 공격자는 서버의 비밀키와 ID를 알 수 없어서 PW를 얻을 수 없다. 만약 공격자가 $RPW = h(r\|PW)$를 얻었다 가정해도 공격자는 사용자가 선택한 random nonce r을 알기 전에 PW를 추측하거나 확인할 수 없다. 따라서 제안된 방식은 오프라인 패스워드 추측 공격에 안전하다.

4.5 User impersonation attack

공격자는 사용자인 것처럼 위장하기 위해서 로그인 요청 메시지를 생성할 수 있어야 한다. 유효한 로그인 요청 메시지 $AID = E_x(ID \oplus h(Y\|b))$를 만들기 위해서 변수 Y값, random number b 그리고 사용자의 ID 정보가 필요하다. 또한 C_u를 생성하기 위해서 $M^* = M$ 같은지 체크해야한다. 하지만 공격자는 변수 Y, b, ID 그리고 $M = h(J\|RPW\|ID)$에 대한 정보를 가지고 있지 않다. 따라서 공격자는 유효한 로그인 요청메시지 $\{AID, T_{u1}, RPW, C_u\}$를 생성하지 못한다. 이러한 이유로 제안된 방식은 사용자 위장 공격에 안전하다.

4.6 DoS(denial of service) attack

제안된 방식은 스마트카드를 작동하기위해 정확한 ID와 PW를 입력해야한다. 스마트카드는 ID와 PW를 이용하여 random nonce $r^* \leftarrow K \oplus h(ID\|PW)$을 찾아오고 $RPW^* \leftarrow h(r^*\|PW)$를 계산한다. 또한 스마트카드에 공유된 secret J를 찾기 위해 먼저 random number $b^* \leftarrow R \oplus h(ID\|x)^*$를 계산하고 $L^* \leftarrow A \oplus h(ID\|b^*)$를 찾아내고 $J^* \leftarrow L^* \oplus h(RPW^*\|b^*)$을 찾아온다. J값을 이용하여 $M^* = h(J^*\|RPW^*\|ID)$를 계산하고 $M^* = M$을

체크하고 값이 같다면 다음세션으로 넘어가고 값이 다르다면 사용자의 요청은 거부된다. 따라서 제안된 방식은 DoS 공격을 완화시킬 수 있다.

4.7 Session key disclosure attack

Kumari 등의 방식과 같이 제안된 프로토콜 안에 사용자와 서버는 공통 세션키 $S_k = h(J \| T_{u1} \| T_{ms2})$를 계산한다. 제안된 방식은 공격자가 공유된 Secret J 값을 얻지 못해 비밀 세션키를 계산하지 못한다. 비록 공격자가 사용자의 current timestamp T_{u1}을 로그인 메시지 $\{AID, RPW, T_{u1}, C_u\}$로부터 쉽게 획득해도 J값을 알지 못하면 서버의 current timestamp T_{ms2}를 얻을 수 없다. 제안된 방식에서 J값을 찾는 것은 Kumari 등의 방식보다 어려워 공격자는 세션키를 계산할 수 없다. 따라서 제안된 방식은 세션키 노출 공격에 안전하다.

4.8 Stolen verifier attack

Kumari 등의 방식과 같이 제안된 방식은 RGR에 등록된 사용자의 ID와 N을 저장한다. N은 서버에 재등록자인지 신규등록자인지 나타낸다. 하지만 Jiang 등의 방식에는 ID를 평문으로 저장하여 취약하지만 Kumari 등의 방식 및 제안된 방식에서는 $\{ID \oplus x, N\}$으로 서버의 비밀키를 사용하여 저장한다. 따라서 비밀키 없이는 저장된 $ID \oplus x$ 로부터 사용자의 ID를 얻을 수 없다. 이와 같이 제안된 방식은 도난 검증 공격에 안전하다.

4.9 Man-in-the-middle attack

Kumari 등의 방식과 같이 제안된 방식은 중간자 공격에 안전하다. 중간 공격자가 공격하기 위해서 서버에게 합법적인 사용자인척하고 사용자에게 유효한 서버인척 해야 한다. 제안된 방식에서 공격자는 서버의 비밀키, 사용자의 ID, random number b 그리고 변수 Y값없이는 AID를 계산할 수 없다. 그리고 응답 메시지 $C_{ms} = E_J(AID \| C_u \| T_{ms2})$를 복호화하기 위한 secret J를 알 수 없다. 따라서 제안된 방식은 Kumari 등의 방식과 같이 서버 위장 공격 및 사용자 위장 공격에 안전하다.

4.10 Privileged insider attack

제안된 방식은 Kumari 등의 방식과 같이 사용자가 PW를 평문으로 보내지 않는다. 사용자는 random nonce r을 사용하여 $RPW = h(r \| PW)$를 서버로 전송하여 서버 내부자는 등록 요청에서 사용자의 PW를 알지 못한다. 또한 해쉬 함수의 일방향 성질에 의해서 $RPW = h(r \| PW)$로부터 PW를 되찾아오는 것은 불가능하다. 따라서 제안된 방식은 권한 내부자 공격에 안전하다.

4.11 Provides user anonymity and user untraceability

제안된 방식에서 사용자의 ID는 스마트카드 안에 평문으로 저장되지 않고 로그인 요청 메시지를 통해 전송되지도 않는다. 공격자가 로그인 요청 메시지를 얻었다고 가정해도 AID를 복호화할 수 없어 사용자의 ID를 얻을 수 없다. 또한 사용자의 스마트카드로부터 사용자의 ID를 되찾아오는 것도 불가능하다. 사용자의 ID는 해쉬 함수의 일방향 설질에 의해서 스마트카드 안에 저장된 정보로부터 되찾아올 수 없다. 또한 서버의 RGR(registration record)에도 평문 ID를 저장하지 않고 비밀키를 사용하여 저장해 ID를 찾는 것은 불가능하다. 이와 같이 제안된 방식은 사용자의 익명성과 불추적성을 제공한다.

4.12 Provides proper mutual authentication

제안된 방식은 Kumari 등의 방식과 같이 양방향 인증을 제공한다. 따라서 단지 서버만 인증하는 것이 아니고 사용자도 서버를 인증할 수 있다. 서버가 사용자로부터 로그인 요청 메시지를 받으면 timestamp T_{u1}을 체크한다. 다음으로 $C_u^* = C_u$가 같은지 체크하고 C_{ms}를 복호화하여 확인한다. 또한 timestamp T_{ms2}도 체크한다. 이와 같이 사용자와 서버는 적절한 상호인증을 통하여 합법적인 서버와 사용자인지 확인한다. 따라서 제안된 방식은 적절한 상호인증을 제공한다.

4.13 Replay attack

제안된 방식은 공격자가 사용자의 로그인 요청 메시지를 엿듣거나 서버의 응답 메시지 C_{ms}를 재전송한다고 가정한다. 각각의 메시지는 timestamp에 의

해서 제한이 된다. 그래서 재전송 공격은 쉽게 time-stamp에 의해 발견된다. 또한 공격자는 timestamp 체크를 우회하거나 피할 수 없다. 따라서 제안된 방식은 재전송 공격에 안전하다.

5. 결 론

원격 환경에서 사용자가 필요한 정보를 안전하게 공유하기 위해서는 순방향 안전성을 제공하는 인증 방식이 요구된다.

본 논문은 원격 환경에서 사용자의 익명성을 보호하며 순방향 안전성을 제공하는 인증 방식을 제안하였다. 제안한 방식은 Kumari 등의 방식과 달리 대칭키를 사용하여 암호화/복호화하여 사용자의 ID를 안전하게 보호하였다. 또한 ID를 이용하여 가상의 ID를 생성하며 가상의 ID는 랜덤 값과 XOR 연산을 통해 사용자의 익명성을 보호한다. Kumari 등의 방식은 순방향 비밀유지, 스마트카드 분실 공격에 취약하다. 하지만 제안한 방식은 Kumari 등의 방식에서 공격자가 비밀키를 획득하게 되면 사용자의 ID를 추측하는 문제점을 개선하여 순방향 안전성을 제공하고 사용자의 ID와 랜덤 값을 서버가 알 수 없도록 새로운 변수를 만들어 전송하므로 스마트카드 분실 공격에 안전한 인증 방식을 제안하였다.

REFERENCE

[1] G. Jaspher, W. Kathrine, E. Kirubakaran, and P. Prakash, "Smart Card Based Remote User Authentication Schemes: a Survey," *Proceeding of International Conference on Modelling Optimization and Computing*, pp. 1318-1326, 2012.

[2] R. Ramasamy and A.P. Muniyandi, "New Remote Mutual Authentication Scheme Using Smart Cards," *Transactions on Data Privacy*, Vol. 2, No. 2, pp. 141-152, 2009.

[3] H.Y. Chien, J.K. Jan, and Y.M. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," *Journal of Computers & Security*, Vol. 21, No. 4, pp. 372-375, 2002.

[4] K.S. Park, S.Y. Lee, Y.H. Park, and Y.H. Park, "An ID-Based Remote User Authentication Scheme in IoT," *Journal of Korea Multimedia Society*, Vol. 18, No. 12, pp. 1483-1491, 2015.

[5] M.K. Khan, S.K. Kim, and K. Alghathbar, "Cryptanalysis and Security Enhancement of a 'More Efficient & Secure Dynamic ID-based Remote User Authentication Scheme," *Journal of Computer Communications*, Vol. 34, No. 3, pp. 305-309, 2011.

[6] Y.Y. Wang, J.Y. Kiu, F.X. Xiao, and J. Dan, "A More Efficient and Secure Dynamic ID-Based Remote User Authentication Scheme," *Journal of Computer Communications*, Vol. 32, No. 4, pp. 583-585, 2009.

[7] H.M. Chen, J.W. Lo, and C.K. Yeh, "An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems," *Journal of Medical Systems*, Vol. 36, No. 6, pp. 3907-3915, 2012.

[8] Q. Jiang, J. Ma, Z. Ma, and G. Li, "A Privacy Enhanced Authentication Scheme for Telecare Medical Information Systems," *Journal of Medical Systems*, Vol. 37, No. 1, pp. 1-18, 2013.

[9] S. Kumari, M.K. Khan, and R. Kumar, "Cryptanalysis and Improvement of 'A Privacy Enhanced Scheme for Telecare Medical Information System'," *Journal of Medical Systems*, Vol. 37, No. 4, pp. 1-11, 2013.

[10] K.W. Kim and J.D. Lee, "On the Security of Two Remote User Authentication Schemes for Telecare Medical Information Systems," *Journal of Medical Systems*, Vol. 38, No. 5, pp. 1-11, 2014.

이 성 엽

2015년 2월 대구한의대학교 IT 콘텐츠학과 학사
2015년 3월 현재 경북대학교 대학원 전자공학부 석사과정
관심분야 : 정보보호, 무선통신보안, 네트워크보안

박 기 성

2015년 2월 경북대학교 산업전자전기공학부 학사
2015년 3월 ~ 현재 경북대학교 대학원 전자공학부 석사과정
관심분야 : 정보보호, 무선통신보안, 네트워크보안

박 요 한

2006년 2월 경북대학교 전자전기컴퓨터 학부 학사
2008년 2월 경북대학교 전자공학과 석사
2008년 3월 ~ 2013년 2월 경북대학교 전자전기컴퓨터학부 박사
2013년 ~ 2014년 National University of Singapore 박사후연구원
2014년 ~ 2015년 경북대학교 산업전자공학과 시간강사
2016년 ~ 현재 경북대학교 전자공학부 박사후연구원
관심분야 : 정보보호, 무선통신보안, 네트워크보안

박 영 호

1989년 2월 경북대학교 전자공학과 학사
1991년 2월 경북대학교 전자공학과 석사
1995년 2월 경북대학교 전자공학과 박사
1996년 ~ 2008년 상주대학교 전자전기공학부 교수
2003년 ~ 2004년 Oregon State Univ. 방문교수
2008년 ~ 2014년 경북대학교 산업전자공학과 교수
2014년 ~ 현재 경북대학교 전자공학부 교수
관심분야 : 정보보호, 네트워크보안, 모바일 컴퓨팅