디지털산업정보학회 논문지 제14권 제4호-2018년 12월
http://dx.doi.org/10.17662/ksdim.2018.14.4.125

퍼지추출 기술을 활용한 스마트 카드 기반 패스워드 인증 스킴*

최 윤 성**

Smart Card Based Password Authentication Scheme using Fuzzy Extraction Technology

Choi Younsung

〈Abstract〉

Lamport firstly suggested password base authentication scheme and then, similar authentication schemes have been studied. Due to the development of Internet network technology, remote user authentication using smart card has been studied. Li et al. analyzed authentication scheme of Chen et al. and then, Li et al. found out the security weakness of Chen et al.'s scheme such forward secrecy and the wrong password login problem, and proposed an a new smart card based user password authentication scheme. But Liu et al. found out that Li et al.'s scheme still had security problems such an insider attack and man-in-the-middle attack and then Liu et al. proposed an efficient and secure smart card based password authentication scheme. This paper analyzed Liu et al.'s authentication and found out that Liu et al.'s authentication has security weakness such as no perfect forward secrecy, off-line password guessing attack, smart-card loss attack, and no anonymity. And then, this paper proposed security enhanced efficient smart card based password authentication scheme using fuzzy extraction technology.

Key Words : Smart Card Security, Password Based Authentication Scheme, Security Analysis

Ⅰ. 서론

네트워크 기술의 발달은 원격지에 위치해있는 다양한 서버와 통신을 가능하게 하였다. 하지만 정당한 사용자가 아닌 악의적인 공격자에 의한 다양한 행위는 정상적인 서비스를 어렵게 하게 있다. 이를 해결하기 위해서 Lamport가 패스워드를 이용한 사용자 인증기법을 제안하고 이후 많은 연구가 진행되었다 [1-3].

Chen 등이 제안한 스마트카드 기반의 패스워드 인증 스킴의 문제점을 Li 등이 분석하여 이를 개선한 스킴을 제안하였다. 하지만 Liu 등은 Li 등의 논문을 분석하여, 중간자 공격과 내부자 공격 등에 취약하며 계산적으로 비효율적이라는 것을 밝혀냈다. 그리고 Lui 등은 자신의 논문에서 제안하는 스킴이 기존의

* 본 논문은 2018년 호원대학교 교비학술연구비 지원과 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1C1B5017492)
** 호원대학교 컴퓨터공학부 사이버보안전공 조교수

스킴에 비해서 효율적은 동작과정을 제공하며, 상호 인증 및 세션 키 동의 과정이 있어 안전하다고 주장했다. 사용자가 원할 때 쉽게 패스워드를 변경할 수 있으며, 재전송 공격, 알려진 키 공격에도 안전하다 주장했다[4-10].

하지만 본 논문에서는 Lui 등이 제안했던 스킴을 분석하여 오프라인 패스워드 추측 공격, 스마트카드 분실 공격에 취약하고 완전 순방향 비밀성 및 익명성을 제공하지 않는다는 것을 밝혀냈다. 그리고 이를 해결하기 위해서 퍼지볼트를 활용해 안전성을 강화한 스마트 카드 기반의 패스워드 인증 기법을 제안하여, 네트워크를 통한 서버와의 통신과정의 안전성을 향상 시키고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 Lui 등이 제안한 스킴의 동작과정을 분석한 후, 3장에서는 Lui 등의 스킴의 안전성 분석을 하여 오프라인 패스워드 추측 공격, 스마트카드 분실 공격에 취약하고 완전 순방향 비밀성 및 익명성을 제공하지 못하는 밝혀낸다. 4장에서는 이러한 문제를 해결하기 위해 본 논문에서 제안하는 인증 스킴의 동작과정을 설명한다. 그리고 5장에서 제안한 스킴의 안전성을 분석하고 기존의 인증 스킴들과 비교하여 안전성이 향상되었다는 것을 증명한다. 6장 결론에서 본 논문의 결론을 짓는다.

Ⅱ. Lui 등의 인증 스킴 분석

2.1 등록 과정

본 논문에서 사용한 용어정보는 <표 1>과 같다. Lui 등의 인증 스킴은 본격적 동작 전에, 서버 S 는 마스터 비밀 키 x 와 일방향 해쉬 함수 $h(\cdot)$를 생성한다.

(1) 사용자 U_i 는 자신의 ID_i, 패스워드 PW_i, 랜덤함수 r 를 선택한 후, $h(r \,||\, PW_i)$를 계산하다. 그리고

<표 1> 용어에 대한 설명

용어	설명
U_i	사용자
S	인증서버
ID_i	사용자 Ui 의 아이디 정보
PW_i	사용자 Ui 의 패스워드 정보
x	서버 S의 마스터 비밀키 정보
T_i	사용자 Ui 의 타임스탬프
T_s	사용자 S 의 타임스탬프
$\triangle T$	타임스탬프의 유효시간
h (·)	일방향 해쉬함수
||	메시지 연결 연산자
$\oplus$	XOR 연산자
sk	공유키
Bio_i	사용자의 생체정보
$Gen()$	생체정보 퍼지 추출기
$Rep()$	생체정보 퍼지 재추출기
R_i	퍼지 추출기에 의해 생성된 랜덤 스트림
P	퍼지 재추출을 도와주는 헬퍼 스트림
a, β	안전하게 생성된 무작위 숫자 정보

사용자는 { ID_i, $h(r \,||\, PW_i)$ }를 비밀 채널을 통해서 서버 S 에게 전달한다.

(2) 서버 S는 아래 파라미터를 생성한다.

$A_i = h(ID_i \oplus x) \,||\, h(x)$,

$B_i = A_i \oplus h(r \,||\, PW_i)$,

$C_i = h(A_i \,||\, ID_i \,||\, h(r \,||\, PW_i))$

(3) 서버 S 는 B_i, C_i, $h(\cdot)$를 새로운 스마트 카드에 저장하고 사용자 U_i 에 안전히 전달한다.

(4) 사용자 U_i 는 r_i 를 스마트카드에 저장한다.

2.2 로그인 과정

본 과정은 사용자가 서버에 로그인하고자 할 때 아래와 같이 이용된다.

(1) 사용자 U_i 는 스마타 카드를 리더기에 넣고 자신의 ID_i 와 패스워드 PW_i 를 입력한다.

(2) 스마트카드는 아래의 파라미터를 계산한다.

$A_i = B_i \oplus h(r \,||\, PW_i)$,

$C_i = h(A_i \,||\, ID_i \,||\, h(r \,||\, PW_i))$.

그리고 스마트카드는 계산된 C_i 와 기존에 저장되어 있는 C_i 를 비교하여 동일하면 이후의 과정을 실행하고 다르면 세션을 닫는다.

(3) 스마트카드는 무작위 넘버 a를 선택한 후 아래와 같은 파라미터를 계산한다.

$D_i = h(ID_i \oplus a)$,

$E_i = A_i \oplus a \oplus T_i$

(4) 스마트카드는 서버 S에게 로그인 요청 메시지를 전송한다.

로그인 요청 메시지 : { ID_i, D_i, E_i, T_i }

2.3 인증 과정

본 과정에서는 사용자와 서버가 상호인증을 완료하고 인증 과정을 마친 후 사용한 세션 키를 계산하고 공유한다. 자세한 과정은 다음과 같다.

(1) 서버 S는 사용자가 보낸 타임 스탬프를 이용하여 시간 유효성을 검사한다.

$T_i - T_i \le \triangle T$

(2) 서버 S는 아래의 파라미터를 계산한다.

$A_i = h(ID_i \oplus x) \,||\, h(x)$,

$a' = E_i \oplus A_i \oplus T_i$,

$D_i' = h(ID_i \oplus a')$.

그리고 난후, 서버는 전달받은 D_i와 계산한 D'_i를 계산한 후, 같으면 인증과정을 계속 진행한다.

(3) 서버 S는 무작위 넘버 r을 선택하고 아래의 파라미터를 계산한다.

$F_i = h(ID_i \oplus \beta)$,

$G_i = A_i \oplus \beta'$.

(4) 서버 S는 사용자에게 인증 메시지 { F_i, G_i, T_s }를 전송한다.

(5) 사용자는 전송받은 메시지에서 타임스탬프를 확인한다.

$T_s - T_s \le \triangle T$

(6) 사용자는 다음 파라미터를 계산한다.

$\beta' = G_i \oplus A_i' \oplus T_s$,

$F_i' = h(ID_i \oplus \beta')$.

그리고 서버는 계산한 F_i 와 전송받은 F_i' 를 비교하여 동일하면 다음 과정을 진행한다.

(7) 사용자 U_i 와 서버 S 는 아래와 같은 세션 키 sk를 계산하고 다음의 보안통신에 이용한다.

$sk = h(a \,||\, \beta' \,||\, h(A_i' \oplus ID_i))$

$= h(a' \,||\, \beta \,||\, h(A_i' \oplus ID_i))$

2.4 패스워드 변경과정

Lui 등이 제안한 스킴은 자유롭게 패스워드를 변경할 수 할 수 있으며 과정은 다음과 같다.

(1) 사용자는 자신의 스마트카드를 넣고 자신의 ID_i, 현재 패스워드 PW_i 를 입력한다.

(2) 스마트카드는 아래의 파라미터를 계산하다.

$A_i^* = B_i \oplus h(r \,||\, PW_i)$,

$C_i^* = h(A_i^* \,||\, ID_i \,||\, h(r \,||\, PW_i))$.

스마트카드는 C_i 와 C_i^* 를 비교하여 동일하면, 사용자는 새로운 패스워드 PW_{inew} 를 입력한다.

(3) 스마트카드는 아래와 같은 파라미터를 생성하여 스마트카드에 저장된 값과 변경한다.

$B_{inew} = A_i^* \oplus h(r \,||\, PW_{inew})$,

$C_{inew} = h(A_i^* \,||\, ID_i \,||\, h(r \,||\, PW_{inew}))$.

Ⅲ. LIU 등의 스킴의 취약성 분석

본 논문에서는 Liu 등의 동작과정을 분석하여 오프라인 패스워드 추측 공격, 스마트카드 분실 공격, 완전 순방향 비밀성 미충족, 익명성 미충족의 문제점이 있다.

3.1 오프라인 패스워드 추측 공격

사용자의 스마트카드에는 B_i , C_i , r , $h(\cdot)$가 저장되어 있고 ID_i는 사용자와 서버간의 통신 상에서 알아낼 수 있다. 저장된 정보는 스마트 카드에 대한 물리 모니터링 방법으로 분석해 낼 수 있다. 그래서 공격자는 ID_i, B_i , C_i , r , $h(\cdot)$를 알고 있어서 다음과 같은 공식을 만들어낼 수 있다.

$C_i = h(A_i' \,||\, ID_i \,||\, h(r \,||\, PW_i))$,
$A_i = B_i \oplus h(r \,||\, PW_i)$,
$\rightarrow C_i = h (B_i \oplus h(r||PW_i) \,||\, ID_i \,||\, h(r||PW_i))$.

C_i 공식에서 공격자는 패스워드 PW_i 를 제외한 모든 정보를 알고 있어 무작위 PW_i 값을 입력하여 동일해질 때까지의 PW_i 값을 알아낼 수 있다.

3.2 스마트카드 분실 공격

Lui 등의 스킴에서 공격자가 사용자의 스마트카드를 습득하게 되면, 공격자는 서버에 로그인하고 인증을 받을 수 있으며 세션 키를 생성할 수 있게 된다. 공격자가 서버와 세션 키를 공유할 수 있게 되는 것은 심각한 문제이며 방식은 다음과 같다. 공격자는 사용자와 서버간의 통신에서 ID_i를 알아내고 스마트카드에서 B_i , C_i , r , $h(\cdot)$를 알아내고 오프라인 패스워드 추측 공격으로 PW_i를 알아낸다. 공격자가 사용자의 스마트카드를 리더기에 넣고 알아낸 ID_i와 PW_i를 입력한다. 스마트카드는 ID_i , PW_i , B_i , C_i , r를 이용하여 A_i , C_i , D_i , E_i와 공격자의 무작위 정보 α를 계산한다. 그 후 공격자가 ID_i, D_i, E_i, T_i를 서버에 전송한다. 그러나 서버는 공격자와 정상적인 사용자를 구분할 수 없다. 서버는 A_i, a, D_i', F_i , G_i를 생성하고 β를 선택한 후, F_i, G_i, T_s를 공격자에게 전송한다. 그리면 공격자는 $sk = h(a \,||\, \beta' \,||\, h(A_i' \oplus ID_i))$를 생성해 낼 수 있으며, 공격자는 sk를 이용하여 향후에도 서버와 비밀통신을 할 수 있다[11].

3.3 완전 순방향 비밀성 미충족

완전 순방향 비밀성일 총족된다는 것은 오랜 기간 사용되는 마스터 키 중 하나가 누출되었을 때, 마스터 키를 이용하여 만들어지는 세션 키를 계산해 낼 수 없는 것을 뜻한다. 하지만 Liu 등의 스킴에서는 완전 순방향 비밀성을 충족하지 않는다. 공격자는 이전 사용자와 서버간의 통신에서 ID_i , E_{Pi} , G_{Pi} , T_{Pi} and T_{Ps}를 알아낼 수 있다. 만약 공격자의 마스터 키 중 하나인 A_i를 알면 다음과 같이 a, β를 알아낼 수 있다.

$a = E_{Pi} \oplus A_i \oplus T_{Pi}$,
$\beta = G_{Pi} \oplus A_i \oplus T_{Ps}$,

그리고 a, β를 이용하여 공격자는 세션키 sk를 알아낼 수 있다.

$sk_P = h(a \,||\, \beta \,||\, h(A_i \oplus ID_i))$

3.4 익명성 미충족

Lui 등의 인증스킴은 익명성을 제공하지 않는다. 이 스킴에서는 사용자가 자신의 ID_i 를 서버 S에게 전송한다. 하지만 이때 ID_i를 어떠한 보호없이 범용 네트워크 환경에서 전송된다. 이렇게 되면, 공격자는 사용자가 서버와 통신하는 과정을 지켜보면서 다양한 정보를 획득할 수 있게 된다. 예를 들어 해당 사용자가 어떠한 서버와 통신을 하는지, 몇 번의 통신을 하는지 등을 알 수 있게 된다. 그러므로 공격자가 사용자를 특정할 수 없도록 ID_i에 보호하여 전송할 필요가 있다.

Ⅳ. 제안하는 인증스킴

Lui 등이 제안했던 스킴의 문제를 해결하기 위해서 본 논문에서는 제안하는 퍼지추출 기겁과 ID 보호 기술을 활용하였다. 퍼지추출 기법(Fuzzy extraction)을 이용하면 생체정보를 랜덤 스트링으로 변경하여 암호학적으로 안전하게 활용하는 것이다. 이 방식은 *Gen*(Generate)와 *Rep*(Reproduce)이라는 효율적인 생성자들로 구성되어 있으며 $Gen(B) = (R, P)$ 에서 생체정보 B 를 이용하여 정규화된 랜덤 스트링 R과 핼퍼 스트링 P 를 생성한다. 그래서 $R = Rep(B', P)$ 에서 사용자가 조금 다른 B' 를 입력하더라도 P 를 이용하여 정상적인 R 을 생성해낼 수 있는 것이다. 퍼지추출 기법을 이용한 인증 스킴에서는 등록 단계에서 R과 P 를 생성하고 로그인 절차에서 P 를 이용하여 정상적인 R 를 도출해내므로, 상황에 따라 조금씩 달라지는 생체정보도 정상적으로 로그인할 수 있게 할 수 있다[10-18].

4.1 등록 과정

본 논문에서 제안하는 인증 스킴은 본격적인 동작 전에, 서버 S 는 마스터 비밀 키 x와 일방향 해쉬 함수 $h(\cdot)$를 준비한다.

(1) 사용자 U_i 는 자신의 ID_i, 패스워드 PW_i 를 입력하고 바이오정보 BIO_i를 추출한다.

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

(2)랜덤함수 r를 선택한 후, $h(r||PW_i || R_i)$를 계산하다. 그리고 사용자는 $\{ h(ID_i), h(r || PW_i || R_i) \}$를 비밀 채널을 통해서 서버 S 에게 전달한다.

(3) 서버 S 는 아래 파라미터를 생성한다.

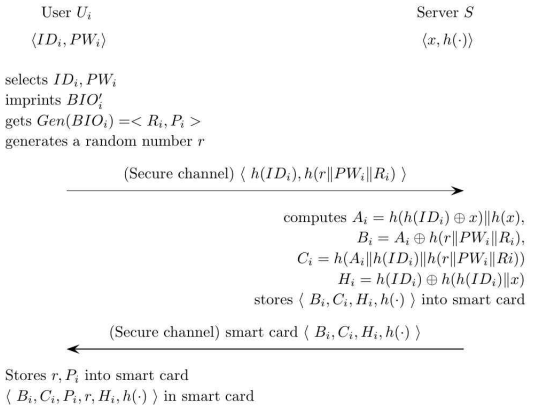
$A_i = h(h(ID_i) \oplus x) || h(x)$,

$B_i = A_i \oplus h(r || PW_i || R_i)$,

$C_i = h(A_i || ID_i || h(r || PW_i || R_i))$

(4) 서버 S는 B_i, C_i, $h(\cdot)$를 새로운 스마트 카드에 저장하고 사용자 U_i 에 안전히 전달한다.

(5) 사용자는 P_i, r_i를 스마트카드에 저장한다.



<그림 1> 제안하는 스킴의 등록과정

4.2 로그인 과정

본 과정은 사용자가 서버에 로그인하고자 할 때 아래와 같이 이용된다.

(1) 사용자 U_i는 스마타 카드를 리더기에 넣고 자신의 ID_i와 패스워드 PW_i 를 입력하고, 자신의 퍼지정보 BIO_i'를 추출하고 R_i 값을 구한다.

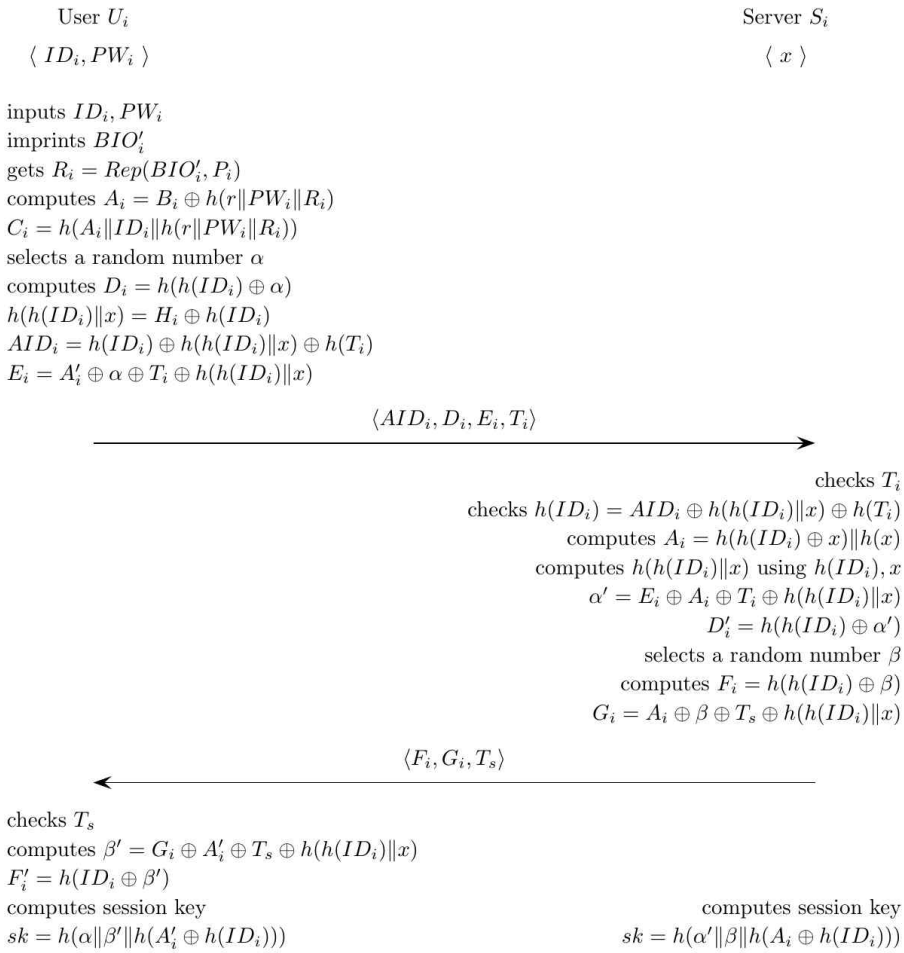
$R_i = Rep(BIO_i', P_i)$

(2) 스마트카드는 아래의 파라미터를 계산한다.

$A_i = B_i \oplus h(r || PW_i || R_i)$,

$C_i = h(A_i || ID_i || h(r || PW_i || R_i))$.

그리고 스마트카드는 계산된 C_i 와 기존에 저장되어 있는 C_i 를 비교하여 동일하면 이후의 과정을 실행하고 다르면 세션을 닫는다.



<그림 2) 제안하는 스킴의 로그인 및 인증과정

(3) 스마트카드는 무작위 넘버 a를 선택한 후 아래와 같은 파라미터를 계산한다.

$D_i = h(h(ID_i) \oplus a)$,

$h(h(ID_i) || x) = H_i \oplus h(ID_i)$

$AID_i = h(ID_i) \oplus h(h(ID_i) || x) \oplus h(T_i)$

$E_i = A_i \oplus a \oplus T_i$

(4) 스마트카드는 서버 S에게 로그인 요청 메시지 $\{AID_i, D_i, E_i, T_i\}$를 전송한다.

4.3 인증 과정

본 과정에서는 사용자와 서버가 상호인증을 완료하고 인증 과정을 마친 후 사용한 세션 키를 계산하고 공유한다. 자세한 과정은 다음과 같다.

(1) 서버 S는 사용자가 보낸 타임 스탬프를 이용하여 시간 유효성을 검사한다. $T_i - T_i \leq \triangle T$

(2) 서버 S는 아래의 파라미터를 계산한다.

$h(ID_i) = AID_i \oplus h(h(ID_i) || x) \oplus h(T_i)$

$A_i = h(h(ID_i) \oplus x) \,||\, h(x)$,
$a' = E_i \oplus A_i \oplus T_i$,
$D'_i = h(h(ID_i) \oplus a')$.

그리고 난후, 서버는 전달받은 D_i와 계산한 D'_i를 계산한 후, 같으면 인증과정을 계속 진행한다.

(3) 서버 S는 무작위 넘버 r을 선택하고 아래의 파라미터를 계산한다.

$F_i = h(h(ID_i) \oplus \beta)$, $G_i = A_i \oplus \beta' \oplus T_s$

(4) 서버 S는 사용자에게 인증 메시지 $\{F_i, G_i, T_s\}$를 전송한다.

(5) 사용자는 전송받은 메시지에서 타임스탬프를 확인한다. $T_s - T_s \leq \triangle T$

(6) 사용자는 다음 파라미터를 계산한다.

$\beta' = G_i \oplus A'_i \oplus T_s$,
$F'_i = h(h(ID_i) \oplus \beta')$.

그리고 서버는 계산한 F_i와 전송받은 F'_i를 비교하여 동일하면 다음 과정을 진행한다.

(7) 사용자 U_i와 서버 S는 아래와 같은 세션키 sk를 계산하고 다음의 보안통신에 이용한다.

$sk = h(a \,||\, \beta' \,||\, h(A'_i \oplus h(ID_i)))$
$= h(a' \,||\, \beta \,||\, h(A'_i \oplus h(ID_i)))$

4.4 패스워드 변경과정

Lui 등이 제안한 스킴은 자유롭게 패스워드를 변경할 수 할 수 있으며 과정은 다음과 같다.

(1) 사용자는 자신의 스마트카드를 넣고 자신의 ID_i, 현재 패스워드 PW_i를 입력하고 바이오정보 BIO_i를 추출하고 R_i 값을 구한다.

$R_i = Rep(BIO_i, P_i)$

(2) 스마트카드는 아래의 파라미터를 계산하다.

$A^*_i = B_i \oplus h(r \,||\, PW_i \,||\, R_i)$,
$C^*_i = h(A^*_i \,||\, ID_i \,||\, h(r \,||\, PW_i \,||\, R_i))$.

스마트카드는 C_i와 C^*_i를 비교하여 동일하면, 사용자는 새로운 패스워드 PW_{inew}를 입력한다.

(3) 스마트카드는 아래와 같은 파라미터를 생성하여 스마트카드에 저장된 값과 변경한다.

$B_{inew} = A^*_i \oplus h(r \,||\, PW_{inew} \,||\, R_i)$,
$C_{inew} = h(A^*_i \,||\, ID_i \,||\, h(r \,||\, PW_{inew} \,||\, R_i))$.

Ⅴ. 제안하는 스킴에 대한 안전성 분석

제안하는 스킴의 안전성을 분석하기 위해 기존의 Liu 등의 스킴에서 분석된 취약성 문제를 포함하여 안전성을 분석하였다. 또한 Liu 등이 제안한 스킴뿐만 아니라 Das, Li & Hwang, An 들이 제안한 스킴들에 대한 안전성 분석을 하였다[4,11].

<표 2> 안전성 분석

안전성 분석	Das	Li & Hwang	An	Liu	제안한 스킴
①	X	X	O	O	O
②	X	X	X	O	O
③	O	O	X	O	O
④	X	O	O	X	O
⑤	X	O	O	X	O
⑥	X	X	X	X	O
⑦	X	X	X	X	O

① 상호인증 : 제안하는 스킴은 다음과 같은 방식으로 상호인증을 제공한다. 서버는 사용자가 보내온 $\{AID_i, D_i, E_i, T_i\}$ 중에서 $h(ID_i) = AID_i \oplus h(x) \oplus h(T_i)$로 $h(ID_i)$를 알아낸 후, $a' = E_i \oplus A_i \oplus T_i$로 a'를 계산한 뒤, $D'_i = h(h(ID_i) \oplus a')$를 계산하여 전송해

온 D_i와 비교함으로서 인증한다. 사용자는 서버가 전송해온 { F_i, G_i, T_s }를 이용하여 $\beta' = G_i \oplus A'_i \oplus T_s$를 계산한 후, $F'_i = h(h(ID_i) \oplus \beta'$를 계산하여 전송해온 F_i와 비교, 동일성을 체크하여 인증하게 된다.

② 세션키 합의 : 제안하는 스킴에서는 등록 및 인증과정을 마친 후에 향후에 사용할 세션키를 만들 수 있다. 사용자는 서버가 전송해온 값을 이용하여 β′을 구한 뒤, $sk = h(a \| \beta' \| h(A'_i \oplus h(ID_i)))$를 구한다. 서버는 사용자가 전송해온 값을 이용하여 a, $h(ID_i)$, A'_i 값을 계산하여 $sk = h(a' \| \beta \| h(A'_i \oplus h(ID_i)))$로 사용자와 동일한 키를 만든다.

③ 자유로운 패스워드 변경 : 제안하는 스킴에는 자신이 원할 때 언제나 패스워드를 변경할 수 있다. 사용자는 패스워드가 누출되었다고 판단되었을 때, 자신의 ID_i, PW_i, PW_{inew}, BIO_i 를 입력하여 스마트카드에 저장된 Bi와 Ci 파리미터를 변경함으로써 패스워드를 변경한다.

$B_{inew} = A^*_i \oplus h(r \| PW_{inew} \| R_i)$,

$C_{inew} = h(A^*_i \| ID_i \| h(r \| PW_{inew} \| R_i))$.

④ 오프라인 패스워드 추측 공격 안전성 : 제안하는 스킴에서는 오프라인으로 패스워드를 알아내기 어렵게 하기 위해서 바이오정보를 이용하였다. 스마트카드 안에 저장된 값들은 전력 모니터링 분석 방식으로 알아낼 수 있다. 그럼에도 불구하고 제안하는 스킴에서는 스마트카드 안에 { B_i, C_i, $h(\cdot)$, P_i, r_i } 값이 들어있는데, $B_i = A_i \oplus h(r \| PW_i \| R_i)$, $C_i = h(A_i \| ID_i \| h(r \| PW_i \| R_i))$에 PW_i 정보가 포함되어있다. 하지만 PW_i 값을 알아내기 위해서는 R_i 값을 알아내어야 한다. 하지만, R_i 값은 사용자의 BIO_i 값을 알아내어야 하기 때문에 공격자가 패스워드 값을 알아낼 수 없다.

⑤ 스마트카드 분실 공격 안전성 : 제안하는 스킴에서는 사용자가 스마트카드를 분실하더라도 공격자가 스마트카드를 이용하여 서버에 인증하고 향후에 사용될 세션 키를 계산할 수 없다. 그 이유는 세션 키를 구성하고 있는 $sk = h(a' \| \beta \| h(A'_i \oplus h(ID_i)))$ 중에서 공격자는 사용자의 $h(ID_i)$을 알아낼 수 없다. 또한, a, β, A_i 값도 사용자의 PW_i 와 BIO_i 정보가 있어야만 생성해낼 수 있기 때문이다. 그러므로 본 스킴은 스마트 카드를 분실하더라도 세션 키 노출에는 안전성을 지닌다.

⑥ 완전 순방향 비밀성 충족 : 본 스킴에서는 공격자는 이전 사용자와 서버간의 통신에서 ID_i , E_{Pi} , G_{Pi} , T_{Pi} and T_{Ps} 를 알아내더라도 sk 값을 알아낼 수 없다. 만약 공격자의 마스터 키 중 하나인 A_i를 알면 다음과 같이 a, β를 알아낼 수 없는 것이다.

$a = E_{Pi} \oplus A_i \oplus T_{Pi} \oplus h(ID_i \| x)$,

$\beta = G_{Pi} \oplus A_i \oplus T_{Ps} \oplus h(ID_i \| x)$.

그리고 a, β를 계산해야지만 공격자는 세션 키 sk를 알아낼 수 없는 것이다. a, β를 알아내기 위해서는 $h(ID_i \| x)$ 를 알 수 있어야하나 공격자는 알 수 없다. 그래서 세션 키 sk 를 알아낼 수 없다.

$sk_P = h(a \| \beta \| h(A_i \oplus h(ID_i)))$

⑦ 익명성 충족 : 본 논문에서 제안하는 스킴은 공격자가 사용자의 ID_i 를 통신과정에서 알아낼 수 없다. 그것은 통신과정에서 사용하는 $AID_i = h(ID_i) \oplus h(h(ID_i) \| x) \oplus h(T_i)$에서는 ID_i을 알아낼 수 없다. 몇 번의 통신을 하는지 등을 알 수 있기 위해서는 사용자를 특정하여야 하는데 이를 위해서는 $h(ID_i)$ 을 알아내어야 한다. 하지만 본 스킴에서는 공격자가 $h(ID_i)$을 알아내기 위해서는 $h(h(ID_i) \| x)$를 계산해야하지만 어렵기 때문이다.

⑧ 성능분석 : Liu 등이 제안한 스킴에서는 등록과

정에서 4번의 해쉬함수 동작이 필요하다. 그리고 로그인 및 인증과정에서는 12번의 해쉬함수 동작이 필요하며, 패스워드 변경과정에서는 4번의 해쉬함수 동작이 필요하다. 본 논문에서 제안하는 스킴에서는 Liu의 스킴보다 등록과정에서는 1번의 $Gen()$ 함수동작이 추가되었다. 그리고 로그인 및 인증과정에서는 1번의 $Rep()$ 함수동작과 1번의 해쉬함수 동작이 추가되었고, 패스워드 변경과정에서도 1번의 $Rep()$ 함수 동작이 추가되었다. 이를 통해 Liu 등이 제안한 스킴에서 발견된 취약점을 해결하고 보다 안전한 스킴을 완성하였다.

VI. 결 론

본 논문에서는 Lui 등이 제안한 스킴의 취약점을 분석하고 발견된 문제점을 해결하기 위해서 퍼지추출 기술을 활용한 스마트 카드 기반 패스워드 인증 스킴을 제안하였다. 본 논문에서 제안하는 스킴은 기존의 스킴에서 발견한 다양한 취약점을 해결하고 있으며, Lui 등이 제안한 스킴의 취약점인 오프라인 패스워드 추측 공격, 스마트카드 분실 공격, 완전 순방향 비밀성 미충족, 익명성 미충족의 문제점을 해결하였다. 제안한 스킴을 통해 인터넷 네트워크를 통한 서버와의 통신과정이 보다 안전해졌으면 한다.

참고문헌

[1] Chang, C. C., Lee, C. Y., Chiu, Y. C., “Enhanced authentication scheme with anonymity for roaming service in global mobility networks,” Computer Communications, Vol.32, No.4, 2009.

[2] Tzong-Chen, W., & Hung-Sung, S., “Authenticating passwords over an insecure channel,” Computers & Security, Vol.15, No.5, 1996, pp. 431-439.

[3] Lamport, L., “Password authentication with insecure communication,” Communications of the ACM, Vol.24, No.22, 1981, pp. 770-772.

[4] Hwang, M. S., & Li, L. H., “A new remote user authentication scheme using smart cards,” IEEE Transactions on Consumer Electronics, Vol.46, No.1, 2000, pp. 28-30.

[5] Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J., & Won, D., “Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography,” Sensors, Vol.14, No.6, 2014, pp. 10081-10106.

[6] Xu, J., Zhu, W. T., & Feng, D. G., “An improved smart card based password authentication scheme with provable security,” Computer Standards & Interfaces, Vol.31, No.4, 2009, pp. 723-728.

[7] Sood, S. K., Sarje, A. K., & Singh, K., “An improvement of Wang et al.’s authentication scheme using smart cards,” In Communications (NCC), 2010 National Conference, 2010, pp. 1-5,

[8] Chen, B. L., Kuo, W. C., & Wuu, L. C., “Robust smart-card-based remote user password authentication scheme,” International Journal of Communication Systems, Vol.27, No.2, 2014, pp. 377-389.

[9] Li, X., Niu, J., Khan, M. K., & Liao, J, “An enhanced smart card based remote user password authentication scheme,” Journal of Network and Computer Applications, Vol.36, No.5, 2013, pp.1365-1371.

[10] Liu, Y. J., Chang, C. C., & Chang, S. C., “An efficient and secure smart card based password authentication scheme,” International Journal of

Network Security, 2016.

[11] Messerges, T. S., Dabbish, E. A., & Sloan, R. H., “Examining smart-card security under the threat of power analysis attacks,” IEEE transactions on computers, Vol.51, No.5, 2002, pp. 541-552.

[12] Choi, Y., Nam, J., Lee, D., Kim, J., Jung, J., & Won, D, “Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics,” The Scientific World Journal, 2014.

[13] Choi, Y., Nam, J., Lee, Y., Jung, S., & Won, D, “Cryptanalysis of advanced biometric-based user authentication scheme for wireless sensor networks,” In Computer Science and Its Applications, Springer Berlin Heidelberg, 2015, pp. 1367-1375.

[14] Jung, J., Choi, Y., Lee, D., Kim, J., Mun, J., & Won, D., “Cryptanalysis of Dynamic ID-Based User Authentication Scheme Using Smartcards Without Verifier Tables,” In Advances in Computer Science and Ubiquitous Computing, 2015, pp. 45-51.

[15] JT. C.Wu and H. S. Sung, “Authentication passwords over an insecure channel,” Computer and Security, Vol.15, No.5, 1996, pp. 431-439.

[16] 박중오, “스마트 디바이스 기반의 보안성 강화를 위한 접근제어 기법 설계,” 디지털산업정보학회 논문지, 제14권, 제3호, 2018, pp. 11-20.

[17] 이재영, “스마트카드 기반의 사용자 인증 기법에 관한 연구,” 디지털산업정보학회논문지, 제14권, 제2호, 2018년, pp. 27-33.

[18] 양환석, “MANET의 멀티캐스트 환경에서 신뢰성 향상을 위한 계층기반 암호 프로토콜 기법 연구,” 디지털산업정보학회논문지, 제13권, 제3호, 2017년, pp. 43-51.

■ 저자소개 ■

최 윤 성
(Choi Younsung)

2016년 3월~현재
호원대학교 컴퓨터공학부 조교수
(사이버보안전공)
2010년 5월~2013년 4월
육군3사관학교 정보공학과 조교수
2015년 8월 성균관대학교
전자전기컴퓨터공학부 (공학박사)
2007년 8월 성균관대학교
전자전기컴퓨터공학부 (공학석사)
2006년 2월 성균관대 정보통신공학부
(공학학사)
관심분야 : 정보보호, 디지털포렌식,
산업정보보호
E-mail : yschoi@howon.ac.kr

논문접수일 : 2018년 11월 29일
수 정 일 : 2018년 12월 18일
게재확정일 : 2008년 12월 18일