Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1027

효율적인 스마트카드 기반 원격 사용자 인증 스킴의 취약점 분석 및 개선 방안*

김 영 일,† 원 동 호‡
성균관대학교

Security Analysis and Enhancement on Smart card-based Remote User Authentication Scheme Using Hash Function*

Youngil Kim,† Dongho Won‡
Sungkyunkwan University

요 약

2012년 Sonwanshi 등은 스마트카드 기반의 해쉬함수를 이용한 효율적인 원격 사용자 인증 스킴을 제안하였다. 본 논문에서는 Sonwanshi 등이 주장한 바와 달리 제안된 스킴이 offline password guessing attack, server impersonation attack, insider attack, replay attack에 취약하며 세션키 및 프라이버시 문제가 존재함을 보이고, 이를 개선한 스킴을 제안한다. 또한, 제안하는 스킴에 대한 분석과 비교를 통해 제안하는 인증 스킴이 다른 인증 스킴보다 상대적으로 안전하고 효율적인 스킴임을 보인다.

ABSTRACT

In 2012, Sonwanshi et al. suggested an efficient smar card based remote user authentication scheme using hash function. In this paper, we point out that their scheme is vulnerable to offline password guessing attack, sever impersonation attack, insider attack, and replay attack and it has weakness for session key vulnerability and privacy problem. Furthermore, we propose an improved scheme which resolves security flaws and show that the scheme is more secure and efficient than others.

Keywords: Remote User Authentication, Smart Card, Password Guessing Attack, Impersonation Attack

I. 서 론

원격 사용자 인증은 다양한 보안 문제에 노출될 수 있는 오픈 네트워크상에서도 사용자와 원격 서버 간 통신의 기밀성과 무결성을 보장해주는 중요한 역할을 한다. 이러한 원격 사용자 인증에는 주로 사용자의 ID와 패스워드가 이용된다[1]. 하지만 ID와 패스워드로만 구성된 인증 스킴들은 Password guessing attack, Replay attack 등 다양한 보안 공격에 쉽게 노출되었다[2]. 이를 보완하기 위해 추가적인 보안 요소인 스마트카드를 이용한 원격 사용자 인증 스킴들이 제안되었다[3-6]. 최근에는 이외에도 지문, 얼굴, 홍채, 음성인식 등 생체정보를 활용한 연구도 활발히 진행 중이다[7].

2012년 Sonwanshi 등[8]은 해쉬함수 기반의 스마트카드를 이용한 원격 사용자 인증 스킴을 제안하였다. [8]의 스킴은 연산 속도가 빠르고 연산량이 적은 XOR과 일방향 해쉬함수만을 사용하기 때문에 굉장히

접수일(2014년 6월 9일), 수정일(2014년 10월 29일), 게재확정일(2014년 10월 29일)
* 이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2014R1A1A2002775)
† 주저자, yikim@security.re.kr
‡ 교신저자, dhwon@security.re.kr(Corresponding author)

효율적이다. Sonwanshi 등[8]은 제안하는 스킴이 DoS attack, offline password guessing attack, impersonation attack, replay attack, stole smart card attack 등 다양한 공격에 안전하다고 주장하였다. 본 논문에서는 [8]이 주장한 바와 달리 제안된 스킴이 offline password guessing attack, server impersonation attack 등에 취약함을 보이고, 이를 개선한 새로운 스킴을 제안하고자 한다.

본 논문에서 제안한 스킴에서는 생체정보의 정확성 향상을 위해 Fuzzy extraction을 사용한다[9]. Fuzzy extraction은 사용자의 생체 정보를 입력 값으로 생성 과정을 거쳐 특정한 값 R을 생성하고, 이후에 입력된 사용자의 상황에 따라 약간 변형된 생체 정보와 helper 값을 입력으로 재생성 과정을 거쳐 앞서 생성된 특정한 값 R을 생성한다. 이 과정은 지문 인식이나 홍채 인식에서 사용자의 입력을 일치시켜주는 중요한 역할을 한다.

본 논문에서는 two-factor authentication인 스마트카드 기반 원격 사용자 인증 스킴의 보안성을 평가하기 위해 공격자의 능력을 다음과 같이 가정한다[10].

공격자는 로그인 및 인증 단계에서 서버와 사용자 사이의 통신과정을 모두 통제할 수 있다. 즉, 공격자는 서버와 사용자간의 메시지를 도청, 첨가, 수정, 또는 삭제할 수 있다. 공격자는 사용자의 스마트카드를 훔쳐서 Kocher 등[11]과 Messerges 등[12]이 주장한대로 전력소비 모니터링을 통해 그 안에 저장된 비밀정보를 추출하거나 사용자의 패스워드를 획득 할 수 있다. 그러나 두 가지 요소를 모두 갖는 비밀정보 추출과 패스워드 획득을 동시에 수행 할 수는 없다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 Sonwanshi 등[8]이 제안한 스킴을 살펴보고 안전성 분석을 통해 문제점을 제기한다. 3장에서는 [8]의 스킴을 개선하여 제안한 문제점을 해결하고, 4장에서는 개선한 스킴의 안전성을 분석한다. 그리고 5장에서는 결론을 맺는다.

II. Sonwanshi의 인증 스킴 분석

Sonwanshi 등은 해쉬 함수와 XOR 연산만을 사용한 스마트카드 기반의 원격 사용자 인증 스킴을 제안하고 제안한 스킴이 서비스 거부 공격, 오프라인 패스워드 추측 공격, 사용자 위장 공격 등 다양한 공격들에 대해 안전함을 주장하였으나, 그들의 주장과 달리 제안한 스킴은 오프라인 패스워드 추측 공격, 서버 위장 공격 등에 취약하다.

Table 1. Notation

Symbol	Description
U_i	The user i
ID_i	The identity of U_i
TID_i	The temporary identity of U_i
Bio_i	Biometrics template of U_i
$Gen(w)$	Generate procedure of Fuzzy extractor
$Rep(w', P)$	Reproduction procedure of Fuzzy extractor
PW_i	The password of U_i
S	The remote server
X	The permanent secret key of server
T_r	The S's timestamp during registration
T_{u_i}, T_s	The U_i's, S's current timestamp, respectively
N^{u_i}, N^s	The U_i's, S's random nonce, respectively
$\triangle T$	Valid time interval for transmission delay
$\|$	Concatenation
$\oplus$	Bitwise XOR operation
$h(\bullet)$	One-way hash function
$\rightarrow$	Insecure channel
$\Rightarrow$	Secure channel

본 논문에서 관련 연구 및 제안한 스킴에 사용될 용어를 Table 1.에서 정의한다.

2.1 Sonwanshi의 스킴

〈등록 단계〉

(1) U_i는 자신의 ID인 ID_i와 패스워드인 PW_i를 선택하고, PW_i를 이용해서 $h(PW_i)$를 계산하고 $\{ID_i, h(PW_i)\}$를 S에게 안전한 채널을 통해 전송한다.

(2) S는 자신의 비밀키 X와 전송 받은 값들을 이용해서 다음을 계산한다.

$$A_i = h(X \| ID_i)$$
$$B_i = A_i \oplus h(ID_i \| h(PW_i))$$

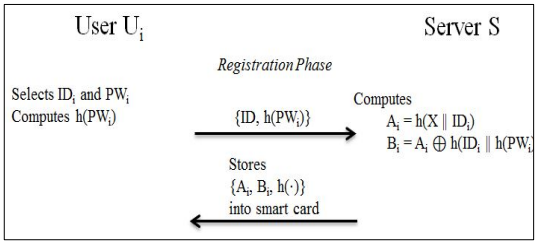


Fig. 1. Registration phase

(3) S는 U_i에게 $\{A_i, B_i, h(\bullet)\}$이 저장된 스마트카드를 발급한다.

〈로그인 단계〉

(1) U_i는 자신의 스마트카드를 카드리더기에 넣고, ID와 패스워드를 입력한다.

(2) 스마트카드는 다음과 같은 수식을 계산한다.

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

(3) 스마트카드는 메모리에 저장되어 있던 값인 B_i와 계산된 값인 B_i^*를 비교하여 값이 같지 않다면 로그인 프로세스를 중단한다.

(4) 값이 같다면 스마트카드는 타임스탬프 값인 T_u를 이용해서 다음 수식을 계산한다.

$$C_{id} = h(PW_i^*) \oplus h(A_i \| T_{u_i})$$
$$E_i = h(B_i \| C_{id} \| T_{u_i})$$

(5) 스마트카드는 사용자 U_i의 로그인 요청 메시지 $\{ID_i, C_{id}, E_i, T_{u_i}\}$를 서버 S에게 전송한다.

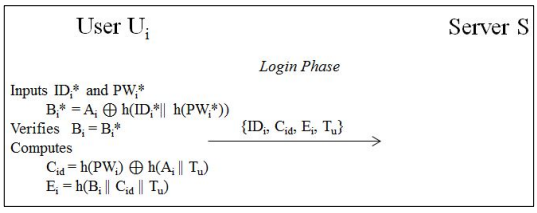


Fig.2. Login phase

〈인증 단계〉

(1) 서버 S는 ID_i와 T_{u_i}의 유효성을 체크한다. T_{u_i}와 전송 받았을 때의 시간 T_{u_i}'간의 차이를 전송 지연시간의 임계값 $\triangle T$와 비교한다.

$$T_{u_i}' - T_{u_i} \leq \triangle T$$

위 식을 만족한다면 다음 과정으로 진행한다. 그렇지 않으면 로그인 요청을 거절한다.

(2) 서버 S는 자신의 비밀키 X와 전송 받은 값들을 이용해서 다음 수식을 계산한다.

$$A_i^* = h(X \| ID_i)$$
$$h(PW_i^*) = C_{id} \oplus h(A_i^* \| T_{u_i})$$
$$E_i^* = h(B_i^* \| C_{id} \| T_{u_i})$$
$$B_i^* = A_i^* \oplus h(ID_i \| h(PW_i^*))$$

(3) 서버 S는 전송 받은 값 E_i와 계산한 값 E_i^*를 비교한다. 값이 다르다면 로그인 요청을 거절한다.

(4) 서버 S는 상호 인증을 위해 다음 수식을 계산한다.

$$F_i = h(A_i^* \| B_i^* \| T_s)$$

서버 S는 계산된 값 F_i를 이용해서 U_i에게 응답 메시지 $\{F_i, T_s\}$를 전송한다.

(5) U_i의 스마트카드는 T_s의 유효성을 체크한다. T_s와 전송 받았을 때의 시간 T_s'간의 차이를 전송 지연시간의 임계값 $\triangle T$와 비교한다.

$$T_s' - T_s \leq \triangle T$$

위 식을 만족한다면 다음 과정으로 진행한다. 그렇지 않으면 로그인 단계로 되돌아간다.

(6) 스마트카드는 다음 수식을 계산한다.

$$F_i^* = h(A_i \| B_i \| T_s)$$

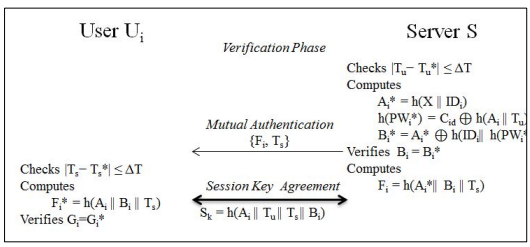


Fig. 3. Verification phase

전송 받은 값 F_i와 계산한 값 F_i^*를 비교한다. 값이 다르다면 로그인 단계로 되돌아간다.

(7) 상호 인증이 성공적으로 완료되면, 사용자 U_i와 서버 S 사이의 세션키 $S_k = h(A_i \| T_{u_i} \| T_s \| B_i)$를 공유한다.

〈패스워드 변경 단계〉

(1) U_i는 자신의 스마트카드를 카드리더기에 넣고 ID와 패스워드를 입력한다.

(2) 스마트카드는 다음과 같은 수식을 계산한다.

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

(3) 스마트카드는 저장되어 있던 B_i와 계산된 B_i^*를 비교한다. 값이 다르다면 패스워드 변경 프로세스를 중단한다.

(4) 스마트카드는 U_i로부터 새로운 패스워드 PW_i^{NEW}를 입력 받고 다음 수식을 계산한다.

$$B_i^{NEW} = A_i \oplus h(ID_i^* \| h(PW_i^{NEW}))$$

스마트카드는 B_i 대신에 계산된 값 B_i^{NEW}를 스마트카드에 저장한다.

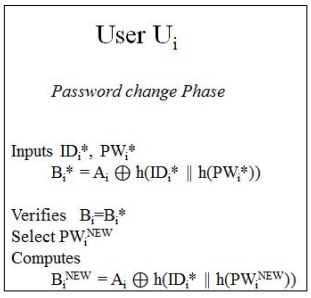


Fig. 4. Password change phase

2.2 Sonwanshi의 스킴 분석

본 장에서는 Sonwanshi 등[8]의 스킴이 offline password guessing attack, server impersonation attack, replay attack, insider attack, replay attack에 취약함을 보이고 세션키의 취약성과 개인 프라이버시 문제에 대해 분석한다.

2.2.1 Offline password guessing attack

공격자 U_a가 사용자 U_i의 스마트카드를 훔치거나 잠시 접근하여 스마트카드를 획득할 수 있다면 다음과 같은 방법으로 U_i의 패스워드를 알아 낼 수 있다[13].

(1) U_a는 획득한 스마트카드에서 전력소비를 모니터링하는 방법으로 사용자 U_i의 숨겨져 있는 비밀정보인 $\{A_i, B_i, h(\bullet)\}$를 추출할 수 있다[11, 12].

(2) U_a는 U_i가 전에 통신한 로그인 요청 메시지를 스니핑하여 ID_i를 알아낼 수 있다.

(3) 패스워드 PW_a를 추측한다.

(4) 추측한 패스워드 PW_a를 이용해서 B_a 값을 계산한다. $B_a = A_i \oplus h(ID_i \| h(PW_a))$.

(5) B_a와 B_i 를 비교한다. 값이 일치한다면, U_a는 패스워드 추측에 성공한 것이다. 그렇지 않다면, U_a는 (3)~(5)를 반복한다.

2.2.2 Server impersonation attack

공격자 U_a가 사용자 U_i에게 잠시 접근하여 스마트카드를 획득할 수 있다면 다음과 같은 방법으로 U_i인척 위장하고 서버 S와 통신할 수 있다.

(1) U_a는 획득한 스마트카드에서 전력소비를 분석하여 사용자 U_i의 비밀정보인 $\{A_i, B_i, h(\bullet)\}$를 추출할 수 있다.

(2) U_a는 U_i의 로그인 요청 메시지$\{ID_i, C_{id}, E_i, T_{u_i}\}$를 가로챌 수 있다.

(3) U_a는 자신의 타임스탬프 T_a를 만들어서 F_a 값을 계산할 수 있다. $F_a = h(A_i \| B_i \| T_a)$.

(4) U_a는 U_i에게 인증 메시지 $\{F_a, T_a\}$를 전송하면 U_i는 정당한 인증 메시지로 간주한다. 즉, 상호 인증이 완료되어 U_a와 U_i간에 세션키를 공유할 수 있다.

2.2.3 Insider attack

서비스를 이용하려는 사용자들은 메일, 메신저, SNS, 은행 업무 등 다른 서비스들을 이용할 때에도 같은 패스워드를 사용하는 경우가 많으므로 사용자의 패스워드가 노출되는 것은 경우에 따라서 굉장히 심각한 문제가 될 수 있다. Sonwanshi 등[8]이 제안한

스킴의 경우, 사용자 U_i는 등록 과정에서 서버 S에게 $h(PW_i)$를 전송하고 이는 패스워드 추측 공격을 통해 U_i의 패스워드를 비교적 빠른 시간 내에 알아낼 수 있게 만든다. 이런 과정을 통해 특권을 가진 서버 S의 내부자는 U_i의 패스워드를 알아낼 수 있다.

2.2.4 Replay attack

Replay attack을 막기 위해 Sonwanshi 등[8]은 전송 지연시간의 임계값 $\triangle T$를 설정했지만, 이는 통신환경이나 통신매체에 따라 큰 변화폭을 갖는다. 따라서 큰 임계값을 갖는 환경에서 공격자 U_a가 임계값보다 빠르게 replay attack을 시도한다면 공격이 가능하다.

2.2.5 Security flaw of session key

[8]의 스킴에서 세션키는 $S_k = h(A_i \| T_u \| T_s \| B_i)$로 이루어져 있다. 이 중에서 A_i와 B_i는 스마트카드 안에 저장된 정보이고, T_u와 T_s는 오픈 네트워크에서 사용자와 서버가 평문으로 통신한다. 따라서 공격자 U_a가 사용자 U_i의 스마트카드를 획득한다면, 이 전에 통신했던 내용을 확인해서 당시 공유했던 세션키 $S_k = h(A_i \| T_{u_i} \| T_s \| B_i)$를 복원할 수 있다. 일반적으로 세션키를 암호화키로 이용해서 안전한 채널을 만들기 때문에, 세션키의 노출은 민감한 정보의 유출로 이어질 수 있다.

2.2.6 Problem about privacy

근래 발생한 IT 보안 사고를 통해 프라이버시에 대한 대중들의 관심이 많아지고 있다. [8]에서는 ID를 오픈 네트워크상에서 평문으로 전송하기 때문에 통신에 참여하지 않는 주체들도 누가 로그인 요청을 하는지, 언제 로그인 요청을 했는지를 모두 알 수 있다. 이를 통해 U_i의 프라이버시가 침해당하는 결과를 초래할 수 있다.

III. 제안 인증 스킴

본 장에서는 Sonwanshi 등[8]이 추구했던 효율성을 유지하면서 보안상 취약점들을 개선한 스킴을 제안한다.

3.1 등록 단계

사용자 U_i는 안전한 채널을 통해 원격서버 S에게 자신의 ID인 ID_i와 생체정보 Bio_i를 전송하고 비밀정보들을 제공받는다.

(1) U_i는 ID_i와 Bio_i를 S에게 전송한다.

(2) S는 ID_i, Bio_i, T_r을 이용해서 다음을 계산한다.

$$Gen(Bio_i) = (R_i, P_i)$$
$$TID_i = h(ID_i \| T_r)$$
$$A_i = h(X \| ID_i)$$

(3) S는 $\{TID_i, A_i, R_i, P_i, h(\bullet)\}$를 U_i에게 전송한다.

(4) U_i는 자신의 패스워드 PW_i를 이용해서 다음을 계산한다.

$$B_i = h(h(ID_i) \oplus h(PW_i \| R_i))$$
$$C_i = A_i \oplus h(ID_i \| PW_i \| R_i)$$

(5) U_i는 $\{TID_i, B_i, C_i, P_i, h(\bullet)\}$를 스마트카드에 저장한다.

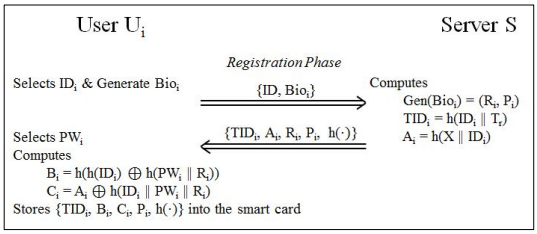


Fig. 5. Registration phase

3.2 로그인 단계

(1) U_i는 자신의 스마트카드를 카드리더기에 넣고 ID_i*와 PW_i*, 생체정보 Bio_i*를 입력한다.

(2) 스마트카드는 U_i가 입력한 생체정보 Bio_i*와 스마트카드에 저장된 P_i로부터 R_i를 추출한다.

$$R_i^* = Rep(Bio_i^*, P_i)$$

(3) 스마트카드는 다음과 같은 수식을 계산한다.

$$B_i^* = h(h(ID_i^*) \oplus h(PW_i^* \| R_i^*))$$

(4) 스마트카드는 B_i^*와 B_i를 비교한다. 만약 같지 않다면 로그인 요청을 중단한다.

(5) 스마트카드는 랜덤으로 N^{u_i}를 선택하고 다음과 같은 수식을 계산한다.

$$A_i = C_i \oplus h(ID_i \| PW_i \| R_i)$$
$$D_i = h(A_i \| N^{u_i} \| h(R_i))$$
$$E_i = N^{u_i} \oplus A_i$$

(6) S에게 $\{TID_i, D_i, E_i\}$를 전송한다.

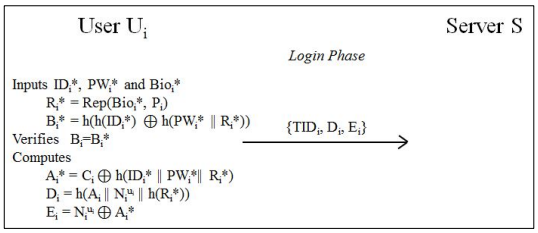


Fig. 6. Login phase

3.3 인증 단계

원격 서버 S는 사용자 U_i로부터 로그인 요청 메시지를 받았을 경우 다음 과정을 수행한다.

(1) TID_i와 E_i의 유효성을 체크한다. 만약 이전에 사용된 TID_i와 E_i라면 로그인 요청을 거절한다.

(2) 인증을 위해 S는 다음 값들을 계산한다.

$$A_i^* = h(X \| ID_i)$$
$$N^{u_i*} = E_i \oplus A_i^*$$
$$D_i^* = h(A_i^* \| N^{u_i*} \| h(R_i))$$

(3) S는 D_i^*와 D_i를 비교한다. 값이 다르다면 로그인 요청을 거절한다.

(4) S는 임의로 N^s를 선택하고 다음과 같이 계산한다.

$$F_i = N^s \oplus A_i^*$$
$$G_i = h(A_i \| N^s \| h(R_i))$$
$$TID_i^{NEW} = h(ID_i \| N^{u_i})$$

(5) S는 TID_i대신에 TID_i^{NEW}를 메모리에 저장한다.

(6) S는 상호인증을 위해 $\{F_i, G_i\}$를 U_i에게 전송한다.

(7) 상호인증 메시지를 전송받은 U_i는 F_i의 유효성을 체크하고 다음과 같은 계산을 한다.

$$N^{s*} = F_i \oplus A_i^*$$
$$G_i^* = h(A_i^* \| N^{s*} \| h(R_i^*))$$

(8) U_i는 G_i^*와 G_i를 비교한다. 만약 같지 않으면 상호인증을 중단한다.

(9) TID_i대신 $TID_i^{NEW} = h(ID_i \| N^{u_i})$를 계산하여 스마트카드에 저장한다.

(10) U_i와 S는 세션키 $S_k = h(A_i \| N^{u_i} \| N^s \| TID_i)$를 공유한다.

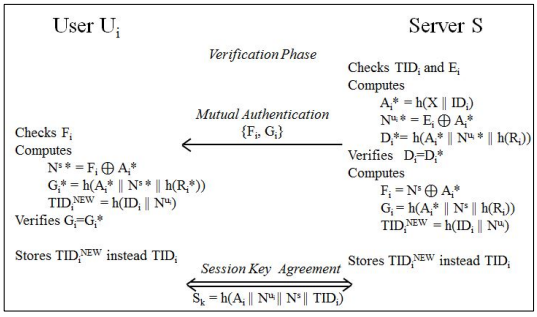


Fig. 7. Verification phase

3.4 패스워드 변경 단계

사용자 U_i가 패스워드를 변경하고 싶을 때, 자신의 스마트카드를 카드리더기에 넣고 ID_i와 PW_i, 생체정보 Bio_i를 입력한 뒤 다음 과정을 거쳐 수행된다.

(1) 스마트카드는 U_i가 입력한 생체정보 Bio_i^*와 스마트카드에 저장된 P_i로부터 R_i를 추출한다.

$$R_i = Rep(Bio_i^*, P_i)$$

(2) U_i는 $B_i^* = h(h(ID_i^*) \oplus h(PW_i^* \| R_i^*))$를 계산하고 B_i와 같은지 비교한다. 만약 값이 다르다면 패스워드 변경을 중단한다.

(2) U_i는 새로운 패스워드 PW_i^{NEW}를 선택한다.

(3) $B_i^{NEW} = h(h(ID_i) \oplus h(PW_i^{NEW} \| R_i))$를 계산하여 기존의 B_i 대신 B_i^{NEW}를 스마트카드에 저장한다.

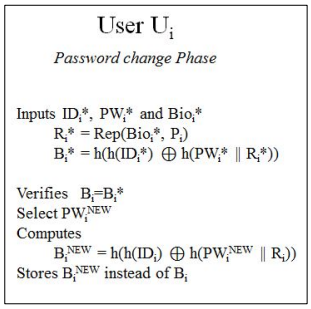


Fig. 8. Password change phase

3.5 스마트카드 폐기 단계

사용자 U_i가 스마트카드 분실을 원격 서버 S에게 폐기를 요청하고 경우에 따라 재발급을 요청한다. U_i는 자신의 ID인 ID_i와 S에 미리 등록된 스스로임을 증명할 수 있는 개인정보들을 안전한 채널을 통해 전송한다. S는 폐기 요청의 유효성을 체크한 뒤, $h(ID_i \| T_c)$를 계산해서 TID_i 대신에 저장한다. 여기서 T_c는 폐기할 때의 타임스탬프이다. 위 과정을 모두 마치면, 로그인 요청 메시지 안의 TID_i가 $h(ID_i \| T_c)$와 같지 않기 때문에 모든 로그인 요청이 거절된다.

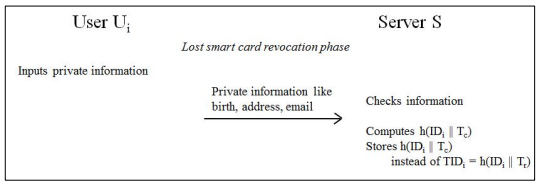


Fig. 9. Revocation of lost smart card phase

IV. 개선된 인증 스킴 분석

본 장에서는 개선된 스킴에 대해 원격 사용자 인증 시스템이 갖춰야 하는 안전성 요구사항에 대해 분석한다[14].

4.1 제안된 인증 스킴 분석

4.1.1 Offline password guessing attack

공격자 U_a가 사용자 U_i의 스마트카드를 획득한다면 [11]과 [12]가 주장한대로 전력소비 공격을 통해 U_i의 비밀정보인 $\{TID_i, B_i, C_i, h(\bullet)\}$를 알 수 있지만, [8]의 스킴과는 달리 제안하는 스킴은 ID가 공개되지 않고 B_i 안에 생체정보인 Bio_i를 이용해 생성된 값이 포함되기 때문에 TID_i와 B_i, C_i를 이용해서 PW_i를 추측하는 것은 어렵다.

4.1.2 Impersonation attack

공격자 U_a가 사용자 U_i인척 원격 서버 S와 통신하기 위해서는 로그인 요청 메시지 $\{TID_i, D_i, E_i\}$를 유효하게 생성할 수 있어야 한다. 하지만 TID_i는 매번 통신할 때마다 바뀌고, U_a가 유효한 TID_i 생성하기 위해서는 그 전에 통신했던 N_i^u를 알아내야 하는데 A_i 값을 알 수 없기 때문에 TID_i를 생성하지 못하며 따라서 사용자 위장 공격이 불가능하다. U_a가 서버 위장 공격을 하기 위해서는 유효한 인증 메시지 $\{F_i, G_i\}$를 생성할 수 있어야 한다. 하지만 U_a가 로그인 요청 메시지를 가로채거나 스마트카드 안의 비밀정보 $\{TID_i, B_i, C_i, h(\bullet)\}$를 안다고 해도 U_i의 생체정보 Bio_i를 이용해서 생성한 값인 R_i과 패스워드 PW_i를 얻을 수 없기 때문에 유효한 인증 메시지를 생성할 수 없고 서버 위장 공격이 불가능하다.

4.1.3 Insider attack

[8]과 달리, 본 논문에서 제안한 스킴에서는 사용자 U_i의 패스워드 PW_i가 어떤 형태로도 원격 서버 S에 전송되지 않는다. 따라서 서버의 내부자는 U_i의 패스워드를 알 수 없다.

4.1.4 Replay attack

공격자 U_a는 사용자 U_i가 원격 서버 S와 오픈 네트워크상에서 주고받는 로그인 요청 메시지 $\{TID_i, D_i, E_i\}$

와 인증 메시지 $\{F_i, G_i\}$를 가로챌 수 있다. 하지만, U_a는 이로부터 유효한 TID_i, E_i, G_i를 생성할 수 없기 때문에 재사용 공격이 불가능하다.

4.1.5 Cryptoanalysis of session key

사용자 U_i의 세션키인 $S_k = h(A_i \| N_i^u \| N_i^s \| TID_i)$에는 오픈 네트워크상에서 전송되지 않고, 스마트카드에 저장되지 않는 값인 A_i와 로그인 요청시마다 업데이트 되는 값인 TID_i가 포함된다. 따라서 이전의 세션키가 노출되거나 U_i의 스마트카드를 통해 비밀정보인 $\{TID_i, B_i, C_i, h(\bullet)\}$가 유출되어도 현재의 세션키는 안전하다.

4.1.6 Problem about privacy

본 논문에서 제안한 스킴에서는 사용자 U_i의 ID인 ID_i가 오픈 네트워크상에서 노출되지 않는다. 또한 이를 대체할 TID_i 값 역시 로그인 요청을 할 때마다 바뀌게 된다. 따라서 공격자 U_a는 통신을 하고 있는 주체에 대한 정보를 전혀 알 수 없기 때문에 U_i의 익명성이 보장되며 U_a의 추적을 방지할 수 있고 이를 통해 프라이버시의 침해 위협을 줄일 수 있다.

4.1.7 Other security problems

공격자 U_a가 원격 서버 S에게 대량의 메시지를 짧은 시간 안에 보내어 S의 업무를 마비 혹은 지연시키는 해킹 기법을 서비스 거부 공격이라고 한다. 본 논문에서 제안하는 스킴에서는 스마트카드 내부에서 사용자 U_i의 적법성을 검사하기 때문에 U_a가 유효하지 않은 메시지를 S에게 전송할 수 없다.

Stolen smart card attack에 대해서는 U_a가 U_i의 ID_i, PW_i뿐 아니라 생체정보인 Bio_i까지 모두 알 수 없으므로 스마트카드를 획득하고 전력소비 모니터링으로 비밀정보를 추출한다고 해도 U_i의 PW_i는 알 수 없다.

또한, 패스워드 변경 단계를 통해서 U_i는 S와 통신하지 않고도 자유롭게 패스워드를 변경할 수 있고, 스마트카드 폐기 단계를 추가함으로써 잃어버린 스마트카드에 대한 보안 위험을 축소시켰다.

4.2 비교분석

본 논문에서 제안한 인증 스킴의 안전성을 검토하기 위해서 Sonwanshi 등[8]이 제안한 인증 스킴을 비롯해서 3개의 스킴과 비교·분석하였다.

Table 2.에서 보이는 바와 같이 [3], [6], [8]의 스킴은 일부 보안 공격 및 위협에 취약한 것을 알 수 있고, 본 논문에서 제안하는 인증 스킴은 이를 개선했음을 알 수 있다.

또한 아래의 Table 3.에서는 사용한 해쉬함수와 XOR 연산을 비롯한 연산 횟수를 비교분석하였다. Table 3.에서 사용된 용어는 다음과 같다.

C_m : mod 연산에서의 지수곱 연산
C_h : 일방향 해쉬 연산

일반적으로 C_m는 C_h에 비해 연산속도가 상당히 느리다.

제안한 논문은 해쉬함수와 XOR연산만을 사용하였으며, 지수곱 연산을 사용한 [3], [6]에 비해 매우 효율적이고, [8]과 비교해도 연산량이 비슷하다.

Table 2. Defensibility in a few schemes

Security threats	[3]	[6]	[8]	Our Scheme
Offline password guessing attack	×	×	×	○
Impersonation attack	×	○	×	○
Insider attack	△	○	×	○
Replay attack	△	○	△	○
Denial of service attack	○	○	○	○
Stolen smart card attack	×	×	×	○
Security flaw of session key	○	○	×	○
Problem about privacy	×	×	×	△
Anonymity	△	×	×	○
Password change phase	○	○	○	○
Revocation of lost smart card phase	×	×	×	○

Table 3. The computational cost of several schemes

	[3]	[6]	[8]	Our Scheme
Low computational cost	$3C_m+1C_h$	$2C_m+1C_h$	$7C_h$	$9C_h$

또한 [8]의 취약점을 해결하여 보다 안전성을 향상시켰기에 의미가 있다.

V. 결 론

Sonwanshi 등[8]이 제안한 스마트카드 기반 원격 사용자 인증 스킴은 XOR연산과 해쉬함수만을 사용하기 때문에 굉장히 효율적이지만, 주장한 바와 달리 다양한 공격에 노출되어 있었다. 본 논문에서는 [8]의 스킴이 offline password guessing attack, server impersonation attack, replay attack, insider attack, replay attack에 취약함을 보이고 세션키의 취약성과 개인 프라이버시 문제가 발생할 수 있음을 보였다. Offline password guessing attack에 선행되는 stolen smart card attack을 막기 위해 스마트카드 폐기 단계를 추가하는 것만으로는 공격을 받은 사용자가 대책을 세우기 전에 모든 정보를 잃어버릴 위험이 있기 때문에, 보안성을 더 향상시키며 기존 스킴의 장점인 효율성을 유지하는 개선된 스킴을 제안하였다. 제안하는 스킴은 익명성을 보장하고 추적을 방지함으로써 프라이버시 위협 역시 효과적으로 감소시켰다. 이러한 스킴은 향후 스마트카드 기반 원격 사용자 인증 스킴 연구에 기여할 것으로 기대된다. 또한 IoT 시대를 맞이할 보안이 향상된 3- factor authentication 연구에 도움이 될 것으로 예상된다.

References

[1] J.H.Nam, K.K.R.Choo, J.H.Kim, H.K. Kang, J.S.Kim, J.R.Paik, and D.H.Won, "Password-only authenticated three-party key exchange with provable security in the standard model," The Scientific World Journal, vol.2014, pp.1-11, Apr. 2014.

[2] M.S.Hwang and L.H.Li. "A new remote user authentication scheme using smart card," IEEE Transaction on consumer Eleclronic, vol. 46, no. 1, pp. 28-30, Feb. 2000.

[3] D. Giri and P.D.Srivastava, "Crypt- analysis and improvement of a remote user authentication scheme using smart cards," International Symposium on Electronic Commerce and Security, pp. 355-361, Aug. 2008.

[4] H. Kai and O. Qingyu, "Cryptanalysis of a remote user authentication scheme using smart cards," 5th International Conference on Wireless Communications, Networking and Mobile Computing 2009, pp. 1-4, Sep. 2009.

[5] J.Y.Kim, D.H.Lee, W.R.Jeon, Y.S. Lee and D.H. Won, "Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks," Sensors 2014, vol. 14, no. 4, pp. 6443-6462, Apr. 2014.

[6] O. Qingyu and H. Kai, "Cryptanalysis and improvement of a remote user authentication scheme," Second International Conference on Intelligent Computation Technology and Automation, vol. 4, pp. 49-52, Oct. 2009.

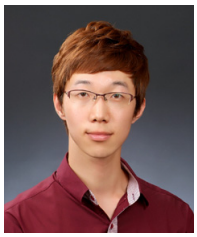
[7] H.B.Tang, Z.J.Zhu, Z.W.Gao, and Y.Li, "A secure biometric-based authentication scheme using smart card," International Conference on Cyberspace Technology, pp. 39-43, Nov. 2013.

[8] S.S. Sonwanshi, R.R. Ahirwal, and Y.K. Jain, "An efficient smart card based remote user authentication scheme using hash function," SCEECS, IEEE Stud. Conf., pp. 1-4, Mar. 2012.

[9] X. Li, J. Niu, M.K. Khan, J. Liao, and X. Zhao, "Robust three-factor remote user authentication scheme with key agreement for multimedia systems," Security and Comm. Networks, pp.1-12, Mar. 2014.

[10] J. Xu, W.T Zhu, and D.G. Feng, "An improved smart card based password authentication scheme with provable security," Computers Standards & Interfaces, vol. 31, no. 4, pp. 723- 728, Jun. 2009.
[11] P.Kocher, J.Jaffe, and B.Jun, "Differential power analysis", Proceedings of Advances in Cryptography (CRYPTO' 99), vol. 1666, pp. 388-397, Dec. 1999.
[12] T.S. Messerges, E.A.Dabbish, and R.H.Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, vol.51, no.5, pp. 541-552, May. 2002.
[13] J.Y.Nam, K.K.R.Choo, M.S.Kim, J.R.Paik, and D.H.Won, "Dictionary attacks against password-based authenticated three-party key exchange protocols", KSII transactions on internet and information systems, vol.7, no.12, pp. 3244-3260, Dec. 2013.
[14] C.T.Li, C.C.Li, C.J.Liu, and C.W.Lee, "A robust remote user authenti- cation scheme against smart card security breach", 25th Annual IFIP WG 11.3 Conference, pp. 231-238, Jul. 2011.

〈저자소개〉



김 영 일 (Youngil Kim) 학생회원
2013년 2월: 성균관대학교 수학과 졸업
2013년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 암호이론, 키 교환 프로토콜, 인증 프로토콜

원 동 호 (Dongho Won) 종신회원
1976년~1988년: 성균관대학교 전자공학과(공학사, 공학석사, 공학박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재: 성균관대학교 전자전기컴퓨터공학과 교수, 한국정보보호학회 명예회장
〈관심분야〉 정보보호, 암호이론, 정보이론