랜덤 Nonce 기반 사용자 인증 스킴의 안전성 개선에 관한 연구

(An Improved User Authentication Scheme Based on Random Nonce)

주 영 도*, 안 영 화**
(Young-Do Joo and Young-Hwa An)

요 약 최근 Yoon 등[7]은 자신이 선택한 패스워드와 스마트카드를 이용하여 원격지에 있는 사용자를 인증할 수 있는 스킴을 제안하였다. 그러나 Yoon 등에 의해 제안된 스킴은 패스워드 기반 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 만족하지 못하고 있다. 본 논문은, 공격자가 사용자의 스마트카드를 훔치거나 일시적으로 접근할 수 있는 경우에 Yoon 등의 스킴은 off-line 패스워드 추측 공격에 취약하다는 것을 증명한다. 그리고 이와 같은 보안 취약점을 해결할 수 있는 hash 함수와 랜덤 nonce 기반의 보다 개선된 인증 스킴을 제안한다. 제안하는 사용자 인증 스킴은 패스워드 추측 공격을 포함한 다양한 공격에 견딜 수 있는 스킴임을 보여주기 위해 보안성 분석을 병행한다. 비교분석 결과에 의하면 제안한 인증 스킴은 무시할 정도의 exclusive-OR 연산의 수행이 조금 더 요구되지만 Yoon 등의 인증 스킴보다 보다 안전하고 효율적인 스킴임을 알 수 있다.

핵심주제어 : 사용자 인증, 스마트 카드, 패스워드 추측 공격

Abstract Recently Yoon et al. proposed the remote user authentication scheme using smart cards. But their scheme has not satisfied security requirements which should be considered in the user authentication scheme using the password based smart card. In this paper, we prove that Yoon et al.'s scheme is vulnerable to a password guessing attack in case that the attacker steals the user's smart card and extracts the information from the smart card. Accordingly, we propose the improved user authentication scheme based on the hash function and random nonce that can withstand various possible attacks including a password guessing attack. The result of comparative analysis demonstrates that the our proposed scheme is much more secure and efficient than the Yoon et al.'s scheme, with a trivial trade-off to require just a few more exclusive-OR operations.

Key Words : User Authentication, Smart Card, Password Guessing Attack

1. 서 론

최근 컴퓨터 네트워크의 급속한 발달과 함께 보안과 인증 기술은 그 중요성이 점점 더 증가하고 있다. 사용자 인증은 비인가된 컴퓨터 접근을 방지할 수 있다. 사용자 인증 프로토콜이란 서비스를 제공하는 서버와 이를 이용하려는 사용자 간에 서로 상대방의 신원을 확인하고 정당한 사용자와 시스템이라는 검증을

* 강남대학교 컴퓨터미디어공학부, 제1저자
** 강남대학교 컴퓨터미디어공학부, 교신저자

수행하는 프로토콜이다[1-8][11-14]. 이와 같은 프로토콜에 의하여 사용자는 사전에 서비스를 제공하는 시스템에 미리 자신의 신원을 확인받을 수 있는 정보를 등록하고, 정당한 사용자임을 검증받고 서비스를 제공받고 싶을 때 언제든지 시스템이 제공하는 서비스를 이용할 수 있다.

1981년에 Lamport[1]는 검증을 위해 리모트 시스템이 패스워드 테이블이 요구되는 패스워드 인증 스킴을 처음으로 제안하였고, 그 이후 패스워드 인증 스킴은 안전성 및 효율성을 개선하기 위해 일부의 연구 방안이 제기 된 바 있다[2,3]. 그러나 이와 같은 인증 스킴들의 취약점은 등록된 사용자의 합법성을 확인하기 위하여 인증 시스템에 검증 테이블이 유지되어야 하는 것이다. 만일 침입자가 서버에 불법적으로 접근할 수 있다면, 검증 테이블의 내용은 쉽게 수정될 수 있을 것이다. 그 이후 이와 같은 문제점을 해결하기 위하여 스마트카드 기반 인증 스킴들이 제안되었다[4-7]. 2000년에 Hwang-Li[4]는 검증 테이블이 필요없는 스마트카드 기반의 새로운 인증 스킴을 제안하였고, 그 후 Hwang-Li의 스킴을 개선한 효율적인 스마트카드 기반 인증 스킴들이 제시되었다[5,6]. 최근에 Yoon 등[7]은 Hwang-Lee-Tang[6]의 인증 스킴을 개선한, 즉 시스템 비밀키 유출과 도용시에도 보안성이 있으며, 사용자와 인증서버 간 상호인증이 가능한 안전하고 효율적인 사용자 인증 스킴을 제안하였다.

일반적으로 스마트카드 기반 사용자 인증 스킴은 인증서버의 오버헤드는 줄이고 사용자는 오직 자신의 패스워드만을 기억할 필요가 있다. 로그인 메시지를 생성하고 전송하는 것 이외에도 스마트카드는 상호인증을 제공한다. 본 논문에서는 스마트카드 기반 사용자 인증 스킴의 안전성을 평가하기 위해 공격자는 다음과 같은 능력을 갖고 있다고 가정한다[8].

- 공격자는 로그인 단계 및 인증 단계에서 서버와 사용자간에 통신과정 모두를 통제할 수 있다. 즉 공격자는 통신과정에서 메시지를 도청, 첨가, 삭제, 또는 수정 할 수 있다.
- 공격자는 (i) 사용자의 스마트카드를 훔쳐서 그 안에 저장되어 있는 내용을 추출하거나 (ii) 또는 사용자의 패스워드를 획득할 수 있다. (iii)그러나 동시에 (i)과 (ii)를 수행할 수 없다.

(i)의 경우, Kocher 등[9]과 Messerges 등[10]은 모든 스마트카드 안에 저장된 비밀정보는 전력소비를 모니터링함으로서 추출할 수 있음을 지적하였다. 따라서 일단 카드를 분실하면 카드 안의 모든 정보는 노출된다.

(iii)의 경우, 사용자가 스마트카드와 자신의 패스워드를 도난당한다면 공격자가 사용자로 위장하는 것을 방지할 수 없다. 따라서 본 논문에서는 스마트카드는 일시적으로 도난당했으나 패스워드는 공격자에게 노출되지 않은 경우에 스마트카드 기반 사용자 인증 스킴에 대해 연구 초점을 두고 있다.

본 논문은 Yoon 등[7]이 제안한 개선된 스킴이 패스워드 추측 공격(password guessing attack)에 취약함을 갖고 있음을 밝혀본다. 즉, 불법적인 공격자가 사용자의 스마트카드에 부당한 방법으로 접근할 수 있다면 스마트카드에 저장된 정보를 추출함으로서 패스워드 추측과 함께 합법적인 시스템 사용자로 가장할 수 있음을 보여준다. 아울러, 본 논문은 Yoon 등이 제안한 스킴의 이러한 보안 취약점들을 개선할 수 있는 스마트카드 기반 인증 스킴을 새로이 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 Yoon 등의 스마트카드를 이용한 사용자 인증 스킴을 기술하고, 안전성을 분석한다. 3장과 4장에서는 개선된 인증 스킴을 새로이 제안하고, 안전성 비교를 통해 Yoon등의 제안에 대한 비교 우위를 입증하고, 5장에서 결론을 맺는다.

2. Yoon 등의 인증 스킴 및 안전성 분석

본 장에서는 Yoon 등[7]이 제안한 스마트카드를 이용한 사용자 인증 스킴을 간단히 기술하고 안전성을 분석한다. 이 스킴은 등록 단계, 로그인 단계, 인증 단계, 그리고 패스워드 변경 단계로 구성된다. 본 논문에서 사용된 표기법은 다음과 같이 정의한다.

U_i : 사용자 i
ID_i : 사용자 i의 아이디
PW_i : 사용자 i의 패스워드
S : 인증 서버
x : 인증 서버의 비밀키
h() : 안전한 일방향 해시 함수
$\oplus$: exclusive-OR 연산자

2.1 Yoon 등의 사용자 인증 스킴

2.1.1 등록 단계

이 단계는 사용자가 인증 서버에 새로이 등록할 때 수행되며 과정은 다음과 같다.

(1) 사용자 U_i는 자신의 아이디 ID_i와 패스워드 PW_i를 선택하고 안전한 채널을 이용하여 인증 서버에 (ID_i, PW_i)를 제출한다.

(2) 사용자의 등록 요청 정보를 수신한 인증 서버 S는 아래와 같이 식 (2.1)과 (2.2)를 계산한다.

$$V_i=h(ID_i, Ttsa, x) \quad (2.1)$$
$$A_i=V_i \oplus PW_i \quad (2.2)$$

여기서, x는 시스템의 비밀키이고, Ttsa는 TSA (time stamp authority)가 제공하는 time stamp이다.

(3) 인증 서버 S는 개별 정보 $\{ID_i, V_i, A_i, h()\}$를 저장한 스마트카드를 사용자에게 발급한다.

2.1.2 로그인 단계

이 단계는 사용자가 로그인하여 인증 서버로부터 인증을 받으려고 할 때 수행된다. 사용자 U_i는 인증 서버에서 발급받은 스마트카드를 카드 리더기에 넣고 아이디 ID_i와 패스워드 PW_i^*를 입력한다. 그리고 나서 스마트카드는 다음 과정을 수행한다.

(1) 스마트카드는 식 (2.3)과 같이 B_i를 계산하고 스마트카드에 저장된 V_i와 비교한다. 만일 값이 같으면 식 (2.4)로부터 C_1를 계산한다. 여기서 T는 입력 장치의 현재 날짜와 시간이다.

$$B_i=A_i \oplus PW_i^* \quad (2.3)$$
$$C_1=h(B_i, T) \quad (2.4)$$

(2) 스마트카드는 사용자 U_i의 로그인 요청 메시지 $\{ID_i, C_1, T\}$를 인증 서버 S에게 전송한다.

2.1.3 인증 단계

인증 요청 메시지 $\{ID_i, C_1, T\}$를 수신한 인증 서버와 스마트카드는 사용자 U_i 와 인증 서버 S 간 상호 인증을 위해 다음 과정을 수행한다.

(1) 인증 서버 S는 ID_i의 형식을 검증한다. 만약 형식이 유효하지 않으면 인증 서버 S는 사용자 U_i의 로그인 요청을 거절한다.

(2) 인증 서버 S는 T와 T′ 사이에 시간 간격의 유효성을 검증한다. 만약 $(T'-T) \geq \Delta T$라면 인증 서버는 로그인 요청을 거절한다. 여기서 ΔT는 유용한 전송 시간이다.

(3) 인증 서버 S는 식 (2.5)와 (2.6)을 계산하고 수신된 C_1과 C_1^*를 비교한다. 만약 값이 같으면 인증 서버는 성공적으로 사용자 U_i를 인증하고 로그인 요청을 받아들인다.

$$B_i=h(ID_i, Ttsa, x) \quad (2.5)$$
$$C_1^*=h(B_i^*, T) \quad (2.6)$$

(4) 인증 서버 S는 식 (2.7)를 계산하고 사용자 U_i에게 메시지 $\{C_2, T''\}$를 전송한다.

$$C_2=h(B_i^*, C_1^*, T'') \quad (2.7)$$

(5) 메시지 $\{C_2, T''\}$를 수신한 사용자 U_i는 T″와 T″ 사이의 시간 간격을 검증한 후, 식 (2.8)를 계산한다.

$$C_2^*=h(B_i, C_1^*, T'') \quad (2.8)$$

만약 $C_2=C_2^*$이면 사용자 U_i는 성공적으로 인증 서버 S를 인증한다.

2.1.4 패스워드 변경 단계

사용자 U_i가 패스워드 PW_i를 새로운 패스워드 PW_i'으로 변경을 요청하고자 하는 경우에는 다음 단계들이 수행된다.

(1) 스마트카드는 $B_i=A_i \oplus PW_i^*(=h(ID_i, Ttsa, x)$를 계산하고 스마트카드에 저장된 V_i와 비교한다.

(2) 만약 같으면, 사용자 U_i는 새로운 패스워드 PW_i'을 선택한다. 그렇지 않으면 패스워드 변경 요청을 거절한다.

(3) $A_i'=B_i \oplus PW_i'$를 계산하고 스마트카드에 저장된 A_i 대신에 A_i'를 저장한다.

2.2 안전성 분석

본 절에서는 Yoon 등의 인증 스킴에 대해 패스워드 추측공격(password guessing attack) 측면에서 안

전성을 분석한다. 이 공격을 수행하기 위해 공격자 U_a는 사용자 U_i의 스마트카드를 훔치거나 일시적으로 접근하여 그 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정한다. 따라서 공격자 U_a는 사용자 U_i의 스마트카드로부터 V_i, A_i, h()를 추출한 후, 다음 단계를 수행하여 사용자의 패스워드를 추측해낼 수 있다.

단계 1: 사용자 U_i는 로그인 요청 메시지 {ID_i, C_1, T}을 생성하여 인증 서버로 전송한다.

단계 2: 이때 공격자 U_a는 사용자 U_i의 로그인 요청 메시지를 가로채서 T와 C_1을 획득한다.

단계 3: 공격자 U_a는 획득한 정보를 이용하여 off-line 패스워드추측 공격을 수행한다.

(1) 공격자 U_a는 사용자 U_i의 패스워드를 PW_i''으로 추측한다.

(2) $C_1''=h(B_i, T)=h(A\oplus PW_i'', T)$를 계산한다.

(3) 계산한 C_1''과 불법 획득한 C_1이 동일한 값인 지를 확인한다.

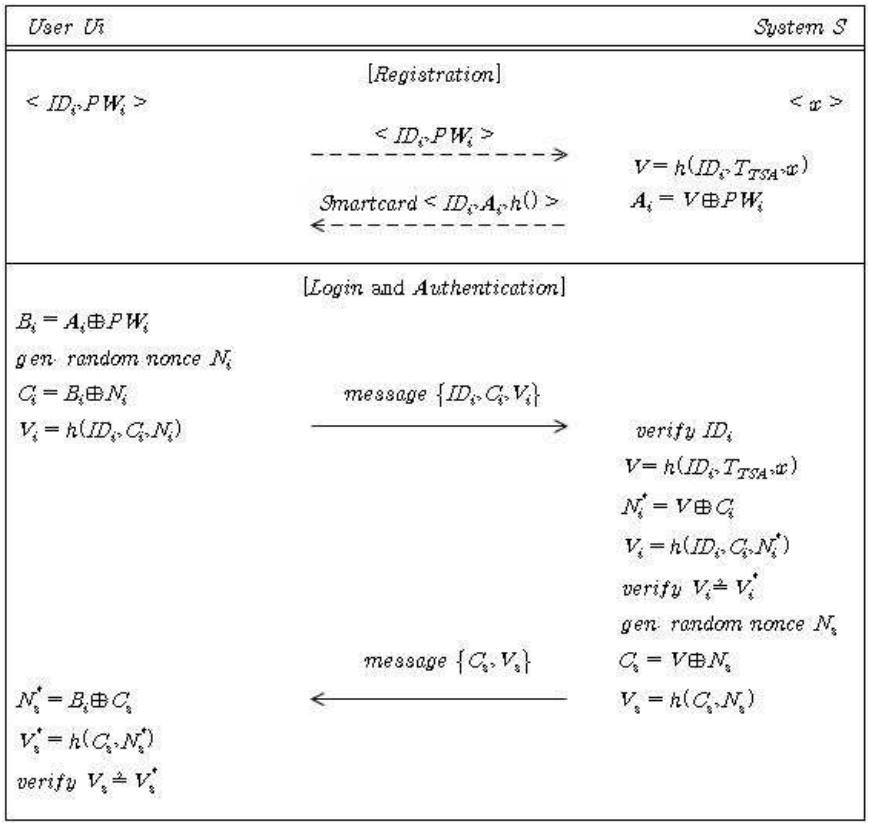
(4) 공격자는 추측한 PW_i''가 (3)의 조건을 만족할 때까지 (1), (2), (3) 과정을 차례로 반복 수행한다. 만족하면 반복 수행을 멈춘다. 따라서 (3)의 조건을 만족하면, 이때 추측된 패스워드 PW_i''은 사용자 U_i의 패스워드이다.

또한, 공격자 U_a는 스마트카드로부터 불법 추출한 A_i, V_i로부터 사용자 U_i의 패스워드를 간단히 알아낼 수 있다. 즉, 수식 (2.1)과 (2.2)로부터 $PW_i=A_i\oplus V_i$ 이므로 용이하게 패스워드를 계산해 낼 수 있다.

이와 같이 Yoon 등의 스마트카드를 이용한 사용자 인증 스킴은 오프라인 패스워드 추측 공격 방식을 이용하면 사용자의 패스워드를 용이하게 찾아 낼 수 있기 때문에 안전성에 취약한 스킴임을 알 수 있다.

3. 제안하는 인증 스킴

본 장에서는 2.2절에서 노출된 바 있는 보안 취약점들을 개선한 새로운 사용자 인증 스킴을 기술한다. 제안하고자 하는 인증 스킴의 안전성은 <그림 1>과 같이 hash 함수와 랜덤 nonce 기반으로 등록 단계, 로그인 단



<그림 1> 제안 인증 스킴

계, 인증 단계, 그리고 패스워드 변경 단계로 구성된다.

3.1 등록 단계

이 단계는 사용자 U_i가 인증 서버 S에 등록하고자 할 때 Yoon 등의 스킴과 유사하게 수행된다.

(1) 사용자 U_i 는 자신의 아이디 ID_i와 패스워드 PW_i를 선택하고 안전한 채널을 이용하여 인증 서버에 (ID_i, PW_i)를 제출한다.

(2) 사용자의 등록 요청 정보를 수신한 인증 서버 S는 다음과 같이 식 (3.1)과 (3.2)를 계산한다.

$$V=h(ID_i, Ttsa, x) \quad (3.1)$$
$$A_i=V\oplus PW_i \quad (3.2)$$

여기서, x는 시스템의 비밀 키이고, Ttsa는 TSA (time stamp authority)에 의해 제공되는 time stamp이다.

(3) 인증 서버 S는 개별 정보 $\{ID_i, A_i, h()\}$를 저장한 스마트카드를 사용자 U_i에게 발급한다.

3.2 로그인 단계

이 단계는 사용자 U_i가 로그인하여 인증 서버에서 인증을 받으려고 할 때마다 수행된다. 사용자 U_i는 스마트카드를 카드 리더기에 넣고 아이디 ID_i와 패스워드 PW_i를 입력한다. 그리고 나서 스마트카드는 다음 과정을 수행한다.

(1) 스마트카드는 다음 식들을 계산한다.

$$B_i=A_i\oplus PW_i \quad (3.3)$$
$$C_i=B_i\oplus N_i \quad (3.4)$$
$$V_i=h(ID_i, C_i, N_i) \quad (3.5)$$

여기서, N_i는 스마트카드에 의해 생성된 랜덤 nonce이다.

(2) 스마트카드는 사용자 U_i의 로그인 요청 메시지 $\{ID_i, C_i, V_i\}$를 인증 서버 S에게 전송한다.

3.3 인증 단계

인증 요청 메시지 $\{ID_i, C_i, V_i\}$를 수신한 인증 서버 S와 스마트카드는 사용자 그리고 인증 서버 간 상호 인증을 위해 다음 과정을 수행한다.

(1) 인증 서버는 ID_i의 형식을 검증하고, 만약 형식이 유효하지 않으면 사용자 U_i의 로그인 요청을 거절한다. 유효하면 인증 서버 S는 다음 식을 계산한다.

$$V=h(ID_i, Ttsa, x) \quad (3.6)$$
$$N_i^*=V\oplus C_i \quad (3.7)$$
$$V_i^*=h(ID_i, C_i, N_i^*) \quad (3.8)$$

만약 $V_i=V_i^*$ 라면, 인증 서버 S는 사용자 U_i를 인증하고 로그인 요청을 받아들인다.

(2) 그런 다음, 인증 서버 S는 랜덤 nonce, N_s를 생성하고 식 (3.9)와 (3.10)를 계산한다.

$$C_s=V\oplus N_s \quad (3.9)$$
$$V_s= h(C_s, N_s) \quad (3.10)$$

(3) 인증 서버 S는 U_i에게 메시지 $\{V_s, C_s\}$를 전송한다.

(4) 서버 인증요청 메시지 $\{V_s, C_s\}$를 수신한 스마트카드는 식 (3.11)과 (3.12)를 계산한다.

$$N_s*=B_i\oplus C_s \quad (3.11)$$
$$V_s^*= h(C_s, Ns^*) \quad (3.12)$$

만약 $V_s=V_s^*$이면 사용자 U_i는 성공적으로 인증 서버 S를 인증한다.

3.4 패스워드 변경 단계

사용자 U_i가 패스워드 PW_i를 새로운 패스워드 PW_i_new로 갱신을 원하는 경우에 다음과 같은 절차가 수행된다.

(1) U_i는 스마트카드를 카드 리더에 넣고 ID_i 및 PW_i를 입력하고 패스워드 변경을 요청한다.

(2) 스마트카드는 인증 서버와의 상호작용에 의해 PW_i의 유용성을 확인하고, 성공하면 사용자 U_i는 새로운 패스워드 PW_i_new를 선택한다.

(3) 스마트카드는 $A_i(=B_i\oplus PW_i)$를 갱신된 A_i_new $(=B_i\oplus PW_i_new)$로 변경하고 저장한다.

4. 제안하는 인증 스킴의 안전성 분석

본 장에서는 제안하고 있는 사용자 인증 스킴에서 패스워드 추측 공격(password guessing attack), 위조 공격(forgery attack), 그리고 재전송 공격(replay attack) 등에 대한 안전성을 분석한다. 그리고 제안한 인증 스킴의 안전성과 계산 복잡도를 Yoon 등[7]의 인증 스킴뿐만 아니라, 기존에 제안된 타 스킴들[5-6]과 비교 분석한다.

4.1 패스워드 추측공격

본 논문에서 다루는 공격자가 패스워드를 획득할 수 있는 방법은 사용자의 스마트카드에 일시적으로 접근하여 스마트카드에 저장된 정보를 추출하고 합법적인 사용자의 메시지를 도청함으로써 감행하는 오프라인 패스워드 추측공격이다. 즉, 합법적인 사용자의 메시지 $\{ID_i, C_i, V_i\}$와 $\{C_s, V_s\}$, 그리고 스마트카드 저장 정보 A_i, h()로부터 패스워드를 추측하는 것이다. 제안하는 스킴의 식 (3.3)과 (3.4)의 $C_i(=B_i \oplus N_i = A_i \oplus PW_i \oplus N_i)$과 식 (3.9)의 $C_s(=V \oplus N_s = h(ID_i, Ttsa, x) \oplus N_s)$로부터 패스워드 PW_i'를 추측하는 것은 랜덤 nonce N_i, N_s 값과 hash 함수 때문에 불가능하다.

4.2 위조공격

공격자는 합법적인 사용자 U_i의 로그인 메시지 $\{ID_i, V_i, C_i\}$를 $\{ID_i, V_s^* C_i^*\}$로 위조하여 인증서버에게 송신한다. 인증 서버는 로그인 사용자를 확인하기 위하여 인증단계를 수행한다. 그러나 이와 같은 위조공격 시도는 인증 단계 식 (3.6), (3.7) 및 (3.8)을 만족하지 못할 것이다. 즉 공격자는 유용한 V_i^*를 계산하기 위하여 $h(ID_i, Ttsa, x)$의 값을 계산 할 수 없다. 왜냐하면, 시스템 파라미터로서 암호학적 키 x를 획득할 수 없기 때문이다.

4.3 재전송 공격

메시지 재전송 공격(replay attack)은 이전 세션의 메시지를 다음 세션에서 재전송하는 방법으로서 불법적인 사용자가 인증을 시도하는 공격이다. 본 논문에서 제안된 인증 스킴은 매 세션마다 새로운 랜덤 nonce N_i, N_s를 생성하기 때문에 공격자는 수식 (3.6)에서 (3.12)에 이르는 인증 단계에서 수행되어져야만 하는 계산을 통과하지 못할 것이다. 따라서 이전 세션의 메시지 정보 $\{ID_i, V_i, C_i\}$와 $\{V_s, C_s\}$를 이용한 재전송 공격은 불가능하다.

4.4 비교 분석

이 절에서는 앞서 기술한 제안 인증 스킴의 안전성과 계산 복잡도를 Yoon 등이 제안한 인증 스킴, 그리고 기존 스킴들과 비교 분석한다.

4.4.1 안전성 분석

본 논문에서 제안한 인증 스킴의 안전성을 분석하기 위하여 안전성 위협요소 및 안전성 향상 요소들을 비교 분석한다.

<표 1>에서 비교된 바와 같이, Yoon 등과 기존 스킴들은 일부 공격, 즉 패스워드 추측공격, 위조공격 등에 취약함을 알 수 있고, 또한 상호인증 기능을 제공하지 않고 있음을 알 수 있다. 그리고 본 논문에서 제안한 인증 스킴은 이와 같은 보안 취약점들을 해결한 개선된 인증 스킴임을 알 수 있다.

<표 1> 안전성 분석

스킴	패스워드 추측공격	위조 공격	재전송 공격	상호 인증
Sun's 스킴[5]	*불가능	불가능	불가능	비제공
Hwang et al's 스킴[6]	가능	가능	불가능	비제공
Yoon et al's 스킴[7]	가능	가능	불가능	가능
제안한 스킴	불가능	불가능	불가능	가능

*시스템에서 사용자에게 패스워드 제공

4.4.2 계산복잡도 분석

본 논문에서 제안한 인증 스킴의 효율성을 분석하기 위하여 인증 스킴의 전 과정에 대해 계산량을 비

교하여 본다. 일반적으로 모든 인증 스킴은 hash와 exclusive-OR 연산을 기반으로 하여 구성되어 있다. exclusive-OR 연산은 매우 적은 계산시간이 요구되기 때문에 일반적으로 그 계산은 무시된다.

<표 2>에 의하면, 본 논문에서 제안한 인증 스킴은 사용자 인증과 관련한 모든 단계에 해당하는 등록단계, 로그인단계, 인증단계 그리고 패스워드 변경단계에 걸쳐 Yoon 등과 기존 스킴들이 제안했던 인증 스킴과 비교하여 exclusive-OR 연산량이 유사하거나 다소 많음을 보여주고 있다. 그러나 계산시간이 적은 연산의 추가에 의해 상대적인 가치가 높은 보안성을 제공할 수 있다는 점에서 상대적으로 효율적인 스킴임을 알 수 있다.

<표 2> 계산량 분석

스킴	등록 단계	로그인 단계	인증 단계	패스워드 변경단계
Sun's 스킴[5]	1T(h)	1T(h)+1T(⊕)	2T(h)+1T(⊕)	비제공
Hwang et al's 스킴[6]	2T(h)+2T(⊕)	2T(h)+2T(⊕)	2T(h)+2T(⊕)	2T(h)+2T(⊕)
Yoon et al's 스킴[7]	1T(h)+1T(⊕)	1T(h)+1T(⊕)	4T(h)	2T(⊕)
제안한 스킴	1T(h)+1T(⊕)	1T(h)+2T(⊕)	4T(h)+3T(⊕)	2T(⊕)

*T(h):hash 연산시간, T(⊕):exclusive-OR 연산시간

5. 결 론

스마트카드를 이용한 사용자 인증 스킴은 공격자가 사용자의 스마트카드 내부에 저장된 정보를 추출하여도 그 정보를 이용하여 사용자의 패스워드를 알아내는데 이용하거나 사용자 또는 서버로 가장할 수 없도록 설계되어야 한다.

본 논문에서는 Yoon 등[7]에 의해 제안된 사용자 인증 스킴은 공격자가 사용자의 스마트카드에 일시적으로 접근하여 저장된 정보를 추출할 수 있다는 가정에서 off-line 패스워드 추측공격이 가능함을 증명하였다. 또한 본 논문에서는 이와 같은 보안 취약점들을 해결한 hash 함수와 랜덤 nonce 기반의 개선된 사용자 인증 스킴을 새로이 제안하였다. 제안한 사용자 인증 스킴은 패스워드 추측공격을 포함한 다양한 공격에 견딜 수 있는 스킴임을 보여 주었다. 비교분석 결과, 제안한 인증 스킴은 Yoon 등과 기존 인증 스킴들보다 기술된 다수의 보안 취약점들을 해결한 효율적인 스킴으로서 상대적으로 exclusive-OR 연산이 다소 더 필요함을 알 수 있다.

따라서 본 논문에서 제안한 사용자 인증 스킴은 기존의 스마트카드 기반 사용자 인증 스킴의 장점을 유지하면서 이전 연구들의 보안상의 문제점들을 효율적으로 해결할 수 있는 스킴으로 스마트카드 기반 사용자 인증 스킴의 연구에 기여할 것으로 기대한다.

참 고 문 헌

[1] L. Lamport, “Password Authentication with Insecure Communication," Communications of the ACM, 24(11), pp. 770-772, 1981.

[2] R. E. Lennon, S. M. Matyas and C. H. Mayer, "Cryptographic Authentication of Time-invariant Quantities," IEEE Trans. Commun., COM-29, Vol. 6, pp. 773-777, 1981.

[3] S. M. Yen and K. H. Liao, "Shared Authentication Token Secure against Replay and Weak Key Attack," Information Proceeding Letters, pp. 78-80, 1997.

[4] M. S. Hwang and L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards," IEEE Trans. Consum. Electron, 46(1), 2000.

[5] H. M. Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards," IEEE Trans. Consum. Electron, 46(4), 2000.

[6] M. S. Hwang, C. C. Lee and Y. L. Tang, "A Simple Remote User Authentication," Math. Comput. Model, 36, pp. 103-107, 2002.

[7] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "An Improvement of Hwang-Lee-Tang's Simple Remote User Authentication," Computer & Security, 24, pp. 50-56, 2005.

[8] J. Xu, W. T. Zhu and D. G. Feng, "An Improved

Smart Card Based Password Authentication Scheme with Provable Security," Computers Standards & Interfaces, 31, pp. 723-728, 2009.
[9] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," Proceedings of Advances in Cryptology (CRYPTO 99), pp. 388 - 397, 1999.
[10] 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, 51 (5), pp. 541 - 552, 2002.
[11] C. W. Lin, C. S. Tsai and M. S. Hwang, "A New Strong-Password Authentication Scheme Using One-Way Hash Functions," Journal of Computer and Systems Sciences International, Vol. 45, No. 4, pp. 623-626, 2006.
[12] X. Duan, J.W. Liu and Q. Zhang, "Security Improvements on Chien et al.'s Remote User Authentication Scheme Using Smart Cards," IEEE International Conference on Computational Intelligence and Security (CIS 2006), 2, pp. 1133-1135, 2006.
[13] 이영숙, 원동호, "스마트카드를 이용한 사용자 인증 스킴의 안전성 분석 및 개선", 한국컴퓨터정보학회 논문지, 제15권, 제1호, pp. 139-147, 2010년 1월.
[14] 안영화, 서정만, "스마트카드를 사용한 원격 사용자 인증 스킴의 시큐리티 개선에 관한 연구", 한국컴퓨터정보학회논문지, 제15권, 제3호, pp. 91-97, 2010년 3월.

주 영 도 (Young-Do Joo)

- 종신회원
- 1983년 : 한양대학교 전자통신공학과 (공학사)
- 1988년 : 미국 University of South Florida 컴퓨터공학과 (공학석사)
- 1995년 : 미국 Florida State University 전산학과 (공학박사)
- 1996년 ~ 2000년 : KT 통신망연구소 연구팀/실장
- 2000년 ~ 2005년 : 시스코 시스템즈 코리아 상무
- 2005년 ~ 2006년 : 화웨이 기술 코리아 부사장
- 2007년 ~ 현재 : 강남대학교 컴퓨터미디어공학부 교수
- 관심분야 : 정보통신, 정보검색, 정보보안

안 영 화 (Young-Hwa An)

- 정회원
- 1990년 2월 : 성균관대학교 전자공학과(공학박사)
- 1983년 3월 ~ 1990년 2월: 해군사관학교 전자공학과 교수
- 1999년 8월 ~ 2001년 7월 : 강남대학교 학술정보처장
- 2002년 3월 ~ 2003년 2월 : Florida State University, 방문교수
- 1990년 3월 ~ 현재 : 강남대학교 컴퓨터미디어공학부 교수
- 관심분야 : 시스템 보안, 네트워크 보안, 정보보안

논 문 접 수 일 : 2010년 07월 29일
1차수정완료일 : 2010년 08월 24일
게 재 확 정 일 : 2010년 08월 26일