Journal of the Korea Academia-Industrial Cooperation Society
Vol. 12, No. 10 pp. 4612-4617, 2011

http://dx.doi.org/10.5762/KAIS.2011.12.10.4612

스마트카드를 이용한 An의 원격 사용자 인증 스킴의 안전성 분석 및 개선

신승수[1*], 한군희[2]
[1]동명대학교 정보보호학과, [2]백석대학교 정보통신학부

Cryptanalysis and Enhancement of the An's Remote User Authentication Scheme using the Smart Cards

Seung-Soo Shin[1*] and Kun-Hee Han[2]
[1]**Dept. of Information Security, College of Information & Communication, Tongmyong University**
[2]**Division of Information & Communication Engineering, Baekseok University**

요 약 Hsiang-Shih는 Yoon등의 스킴을 개선한 사용자 인증 스킴을 제안하였다. 그 후 An은 Hsiang-Shih이 제안한 스킴이 패스워드를 기반으로 하는 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 만족하지 못함을 보였다. 즉, Hsiang-Shih이 제안한 스킴에서 공격자가 사용자의 스마트카드를 훔치거나 일시적으로 접근하여 그 안에 저장된 정보를 추출하여 사용자의 패스워드를 알아낼 수 있음을 보였다. 그러나 An이 제안한 스킴도 패스워드 추측공격, 위조/위장 공격 등에 취약함을 보이고 개선된 사용자 인증 스킴을 제안하였다. 제안한 인증 스킴은 패스워드 추측공격이 불가능하고 사용자와 인증 서버가 상대방을 인증할 수 있는 효율적인 상호 인증방식을 제시하였다.

Abstract Hsiang-Shin proposed a user authentication scheme which was created by improving Yoon's scheme. Afterwards, An showed the failure to meet security requirements which are considered in user authentication using password-based smart card in Hsiang-Shih-suggested scheme. In other words, it was found that an attacker can steal a user's card, and detect a user's password by temporarily accessing it and extracting the information stored in it. However, An-proposed scheme also showed its vulnerability to password-guessing attack and forgery/impersonation attack, etc. and thus, this paper proposed the improved user authentication scheme. The proposed authentication scheme can thwart the password-guessing attack completely and this paper proposed scheme also includes an efficient mutual authentication method that can make it possible for users and authentication server to certify the other party.

Key Words : User Authentication, Smart Cards, Password Guessing Attack, Replay Attack

1. 서론

사용자는 언제 어디서나 다양한 인터넷 서비스를 제공받고자 한다. 또한 분산컴퓨팅 환경에서 원격으로 작업을 수행하는 일이 빈번해지면서 인증에 대한 많은 연구가 진행되고 있다. 그 중 스마트카드를 이용한 원격 사용자 인증은 스마트카드가 지닌 이동성과 기능적 안전성으로 인하여 주목받고 있다.

서비스를 제공하는 서버와 이를 이용하려는 사용자 간에 서로 상대방의 신원을 확인하고 정당한 사용자와 서버라는 검증을 수행하는 프로토콜을 사용자 인증 프로토콜이라 한다. 초기의 인증 프로토콜에서 서버는 사용자 인증 요청에 대한 검증을 위해 검증 테이블을 저장하고 있어야 했다[1]. 하지만 서버에 대한 안전성과 신뢰가 요구되는 사용자의 아이디와 패스워드 관리 부담 등의 문제가 제기되면서 검증테이블을 이용하지 않는 인증 기법들이 연구되고 있다. 2002년 Chien등은 효율적인 패스워드 기반 원격 사용자 인증 스킴을 제안하였다[2]. 이 스킴

*교신저자 : 신승수(shinss@tu.ac.kr)
접수일 11년 09월 05일 수정일 (1차 11년 09월 26일, 2차 11년 10월 01일, 3차 11년 10월 05일) 게재확정일 11년 10월 06월

은 상호인증을 제공하고 검증테이블이 불필요하고 자유로이 패스워드를 변경할 수 있으며, 그리고 오직 소수의 해시연산을 수행한다. 그러나 2004년에 Ku-Chen은 Chien등이 제안한 스킴은 반사공격(reflection attack), 내부자공격(insider attack)에 취약함을 지적하고 이를 개선한 스킴을 제안하였다[3]. 또한, Yoon[4]등은 개선된 스킴이 여전히 병렬 세션공격(parallel session attack)이 의심되며 패스워드 변경단계에서 사용자의 패스워드 변경이 안전하지 못한 것을 지적하고 개선된 스킴을 제시하였다. 그 후, 2008년에 Hsiang-Shih는 Yoon등의 스킴이 Duan등이 기술한 병렬 세션공격에 취약하고[5], 위장공격, 그리고 패스워드 추측공격에도 취약함을 보였으며, 이들 문제점을 개선한 효율적인 스킴을 제안 하였다[6]. 그러나, An[7]은 Hsiang-Shih이 제안한 개선된 스킴도 여전히 패스워드 추측공격 및 위조공격에 취약함을 보이고 이를 개선한 인증 스킴을 제안하였다.

An은 Hsiang-Shih이 제안한 스킴을 개선한 스킴이 패스워드 추측공격 및 위조공격에 안전함을 보이기 위해서 랜덤 값을 이용하여 개선된 스킴을 제안하였다. 그러나 패스워드 추측공격 및 위조공격 등 스마트카드 기반 인증시스템이 갖추어야 하는 안전성 요구 사항을 만족하지 못하고 있다.

본 논문에서는 패스워드 추측공격, 위장공격과 재전송 공격등에 안전하고, 스마트카드 기반 인증시스템이 갖추어야 하는 안전성 요구 사항을 만족하는 개선된 스마트카드기반 인증 스킴을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 An이 제안한 스마트카드를 이용한 원격 사용자 인증 스킴에 대하여 알아보고, 취약성을 분석하였다. 3장에서는 개선된 스킴을 제안하고 4장에서는 개선된 스킴에 대하여 분석하였다. 그리고 5장에서 결론을 맺는다.

2. An의 인증 스킴 분석

An은 공격자가 사용자의 스마트카드에 저장된 정보를 추출한 후 그것을 이용하여 사용자의 패스워드를 알아낼 수 있음을 보였다. Hsiang-Shih의 인증 스킴의 분석 내용과 이를 개선한 An의 인증 스킴에 대하여 알아본다.

본 논문에서는 스마트카드기반 사용자 인증 스킴의 안전성을 분석하기 위하여 공격자는 다음과 같은 공격능력을 갖고 있다고 가정한다[8][9].

(1) 공격자는 서버와 사용자간에 로그인단계 및 인증단계를 모두 통제할 수 있다. 즉, 공격자는 서버와 사용자간에 전달되는 메시지의 내용을 도청, 삭제, 수정 또는 첨가 할 수 있다.

(2) 공격자는 사용자의 스마트카드 안에 내장되어 있는 내용을 추출하거나 또는 사용자의 패스워드를 획득할 수 있다.

따라서 패스워드를 기반으로 하는 스마트카드를 이용한 사용자 인증 스킴의 안전성은 다음 두 가지 상황 중 한 가지만 발생할 때 그 안전성을 보장해야 한다. 만일 (i) 사용자의 스마트카드가 분실된다. (ii) 사용자의 패스워드가 노출된다. 이러한 상황이 모두 발생했을 때는 패스워드를 기반으로 하는 스마트카드를 이용한 어떤 사용자 인증 스킴도 그 안전성을 보장 받을 수 없다.

본 논문에서 관련된 연구 및 제안한 스킴에서 사용될 용어를 표 1과 같이 정의한다.

[표 1] 용어 정의
[Table 1] Notation

기호	설명
U_i	i 번째 사용자
U_a	공격자
ID_i	i 번째 사용자의 아이디
PW_i	i 번째 사용자의 패스워드
S	인증서버
x	인증서버의 비밀키
T_u, T_S	사용자 및 인증서버에 의해 생성된 타임스탬프
h()	안전한 일방향 해시함수
$\|\|$	연접
$\oplus$	XOR 비트 연산자

2.1 Hsiang-Shih 인증 스킴 분석

Kocher[8]와 Messerges[9]가 제안한 논문에서 그들은 스마트카드 안에 저장된 정보를 전력소비 공격 등을 이용해서 추출할 수 있다고 주장하였다. 이런 사실에 근거하여 사용자의 스마트카드를 획득하여 그 안에 저장된 정보를 추출한 공격자는 이를 이용하여 사용자의 패스워드를 알아낼 수 있는 오프라인 패스워드 추측공격을 수행할 수 있다.

이러한 가정에 Hsiang-Shih등이 제안한 스킴은 오프라인 패스워드 추측공격에 취약하다고 An은 다음과 같이 분석을 하였다. 사용자 U의 스마트카드로부터 V, R과 b를 추출한 공격자 U_a는 사용자 U의 패스워드 PW를 알아낼 수 있다. 다음과 같이 진행된다.

1 : 정당한 사용자 U는 인증서버 S에 로그인하기 위해 C_1, C_2를 계산하고, 로그인 요청메시지 {ID, T_u, C_2}를 인증 서버 S에 전송한다.

2 : 공격자 U_a는 사용자 U의 로그인 메시지를 가로채서 T_u와 C_2를 획득한다.

3 : 공격자 U_a는 오프라인(off-line) 패스워드 추측 공격을 아래와 같이 정당한 사용자 U의 패스워드를 알아낼 수 있다.

(1) 공격자 U_a는 정당한 사용자 U의 패스워드를 추측한다.

(2) 공격자 U_a는 가로챈 정보로부터 $C_1'=R\oplus h(b\oplus PW')$, $C_2'=h(C_1'\oplus T_u)$를 계산한다.

(3) 공격자 U_a는 C_2'와 C_2가 동일한 값을 갖는지를 확인한다.

(4) 공격자 U_a는 자신이 추측한 PW'가 (3)의 조건을 만족할 때까지 (1), (2), 그리고 (3) 세 개의 과정을 차례로 반복 수행한다. 만족하면 반복 수행을 멈춘다.

공격자 U_a는 결국 (3)의 조건을 만족하는 PW'를 알아낼 수 있으면, 이 패스워드가 정당한 사용자 U의 올바른 패스워드가 된다. 이와 같이 Hsiang-Shih이 제안한 스마트카드를 이용한 사용자 인증 스킴은 패스워드 추측 공격 방식에 취약하다. 이를 개선하기 위해서 An은 랜덤 값을 이용한 새로운 인증 스킴을 제안하였다.

2.2 개선된 An의 인증 스킴

An의 인증 스킴도 Hsiang-Shih의 인증 스킴의 특성을 유지하며, 등록단계, 로그인단계, 그리고 검증단계로 구성된다.

<등록단계>

이 단계는 사용자 U가 서버 S에 등록하거나 재등록할 때 수행된다, 여기서, n은 사용자 U가 서버 S에 재등록한 횟수를 나타낸다.

(1) 사용자 U는 랜덤 값 b를 선택하고, 패스워드 PW를 이용하여 해시값 $h(b\oplus PW)$를 계산한다.

(2) 사용자 U는 서버 S에게 ID, $h(b\oplus PW)$를 전송한다.

(3) 만약 사용자 U가 초기등록이라면, 서버 S는 사용자 U를 위한 계정 데이터베이스를 생성하고 n=0을 저장한다. 그렇지 않다면 서버 S는 n=n+1로 사용자 U를 위해 항목을 변경한다. 그리고 서버 S는 다음을 계산한다.

$$P=h(EID\oplus x),\quad R=P\oplus h(b\oplus PW)$$

여기서, $EID=(ID\,\|\,n)$이다.

(4) 서버 S는 사용자 U에게 R 그리고 h()이 저장된 스마트카드를 발급한다.

(5) 사용자 U는 b를 스마트카드에 저장한다.

<로그인 단계>

이 단계는 사용자 U가 서버 S에게 로그인을 요청할 때마다 수행된다.

(1) 사용자 U는 스마트카드를 스마트카드 리더기에 넣고 ID와 PW를 입력한다.

(2) 사용자 U의 스마트카드는 다음계산을 수행한다.

$$C_i=R\oplus h(b\oplus PW),\quad C_u=C_i\oplus N_u,$$
$$V_u=h(ID,\ C_u,\ N_u)$$

여기서, N_u는 스마트카드에 의해 선택된 랜덤수이다.

(3) 사용자 U는 서버 S에게 메시지 $M_u=\{ID,\ C_u,\ V_u\}$를 송신한다.

<검증단계>

원격시스템 및 스마트카드는 인증 요청 메시지 $M_u=\{ID,\ C_u,\ V_u\}$을 수신 후에 다음을 수행한다.

(1) 만약 ID가 유효하지 않다면 서버 S는 사용자 U의 로그인 요청을 거절한다. 그렇지 않다면 서버 S는 N_u', V_u'를 계산한다.

$$N_u'=h(EID\oplus x)\oplus C_u,\quad V_u'=h(ID,\ C_u,\ N_u')$$

만약, $V_u=V_u'$이라면 서버 S는 사용자 U를 인증하고 로그인 요청을 받아들인다.

(2) 서버 S는 생성된 랜덤 값 N_s를 생성하여 C_s와 V_s를 계산한다.

$$C_s=h(EID\oplus x)\oplus N_s,\ V_s=h(ID,\ C_u,\ C_s,\ N_s)$$

(3) 서버 S는 사용자 U에게 메시지 $M_u=\{V_s,\ C_s\}$를 전송한다.

(4) 서버 인증 요청 메시지 $M_u=\{V_s,\ C_s\}$를 수신한 사용자 스마트카드는 N_s'과 V_s'를 계산한다.

$$N_s'=C_s\oplus C_i,\quad V_u'=h(ID,\ C_u,\ C_s,\ N_s')$$

만약, $V_s=V_s'$이라면 사용자 U는 성공적으로 서버 S를 인증한다.

2.3 An의 인증 스킴의 분석

An은 Hsiang-Shih에 의해 제안된 스마트카드를 이용한 사용자 인증 스킴이 안전성에 취약함을 보였다. 이와 같은 문제점을 해결하기위해 해시함수와 난수에 기반 한 개선된 사용자 인증 스킴을 제안하였다. 그러나 An의 인증 스킴 역시 안전성에 취약하다.

An은 오프라인 패스워드 추측 공격에 대한 안전성의 문제점을 다음과 같이 분석 하였다. 이 공격을 수행하기 위해 공격자 U_a는 사용자 U_i의 스마트카드를 훔치거나 일시적으로 접근하여 그 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정을 한다. 따라서 사용자 U_i의 스마트카드로부터 R, b, h() 를 추출한 공격자 U_a는 다음

과 같은 단계로 사용자 U_i의 패스워드를 알아낼 수 있다.

단계 1 : U_i는 로그인 요청 메시지 M_u={ID, C_u, V_u}을 생성하여 인증서버로 전송한다.

단계 2 : 이때 공격자 U_a는 U_i의 로그인 요청 메시지를 가로채서 C_u과 V_u를 획득한다.

단계 3 : 공격자 Ua는 획득한 정보를 이용하여 오프라인 패스워드추측 공격을 수행한다.

(1) 공격자 U_a는 U_i의 패스워드 PW_i'로 추측한다.

(2) 스마트카드로부터 추출한 정보 R과 PW_i'로부터 C_i'=R⊕h(b⊕PW')를 계산한다.

(3) 다음은 획득한 C_u를 이용하여 N_u'을 얻는다.

$$C_u \oplus C_i' = N_u'$$

(4) C_i'과 N_u'를 이용하여 V_u'=h(ID, C_u, N_u')를 계산한다.

(5) 계산한 V_u'와 불법 획득한 V_u가 동일한 값인지를 확인한다.

(6) 공격자는 추측한 PW_i'가 (5)의 조건을 만족할 때까지 (1),(2),(3),(4)과정을 차례로 반복 수행한다. 만족하면 반복 수행을 멈춘다. 따라서 (5)의 조건을 만족하면, 이때 추측된 패스워드 PW_i'는 사용자 U_i의 패스워드이다.

An이 제안한 스킴에서 패스워드가 노출되기 때문에 위장공격, 재전송공격에도 취약하다. 따라서, 이러한 공격에 안전하고 An이 제안한 스킴의 특성을 유지하는 개선된 새로운 스킴을 제안한다.

3. 개선된 인증 스킴

An은 Hsiang-Shih이 제안한 인증 스킴이 오프라인 패스워드 추측공격에 취약함을 보이고 랜덤 값을 이용하여 개선된 논문을 제안하였다. 그러나, An의 스킴도 공격자에 의해 패스워드가 노출됨을 보였다.

본 장에서는 An에 의해 제안된 사용자 인증 스킴이 갖고 있는 취약성에 대한 분석 내용을 인증서버의 비밀키와 타임스탬을 이용하여 새로운 스킴을 제안한다. An의 인증 스킴의 특성을 유지하면서 개선된 인증 스킴도 등록단계, 로그인단계, 검증단계로 구성된다.

3.1 등록단계

이 단계는 사용자 U_i가 서버 S에 등록할 때 수행된다.

단계 1 : 사용자 U_i는 랜덤 값 b와 패스워드 PW_i를 선택하고, 해시값 I=h(b⊕PW_i), v=h(b⊕ID_i)을 계산한다.

단계 2 : 사용자 U_i는 서버 S에게 I, v을 안전한 채널로 전송한다.

단계 3 : 만약 사용자 U_i가 초기등록이라면, 서버 S는 사용자 U_i를 위한 계정 데이터베이스를 생성하고 n=0을 저장한다. 그렇지 않다면 서버 S는 n=n+1로 사용자 U_i를 위해 항목을 변경한다. 그리고 서버 S는 다음을 계산한다.

$$P=h(EID \oplus x), \quad R=P \oplus h(b \oplus PW_i)$$

여기서, EID=(v ‖ n)이다.

단계 4 : 서버 S는 사용자 U_i에게 R 그리고 h()이 저장된 스마트카드를 발급한다.

단계 5 : 사용자 U_i는 b를 스마트카드에 저장한다.

3.2 로그인단계

이 단계는 사용자 U_i가 서버 S에게 로그인을 요청할 때마다 실행된다.

단계 1 : 사용자 U_i는 스마트카드를 스마트카드 리더에 넣고 ID_i와 PW_i를 입력한다.

단계 2 : 사용자 U_i의 스마트카드는 다음을 계산한다.

$$C_1=R \oplus h(b \oplus PW_i), \quad C_2=C_1 \oplus h(x) \oplus T_u,$$
$$V_u=h(v, C_2, T_u)$$

여기서, T_u는 사용자 U_i의 현재 타임스탬프이다.

단계 3 : 사용자 U_i는 서버 S에게 인증 요청 메시지 M_u={v, C_2, V_u}를 송신한다.

3.3 검증단계

원격시스템은 인증 요청 메시지 M_u={v, C_2, V_u}를 수신 후에 원격시스템 및 스마트카드는 다음을 수행한다.

단계 1 : 만약, 사용자 U_i의 ID_i가 유효하지 않거나, 또는 T_s-T_u≤0이면 서버 S는 사용자 U_i의 로그인 요청을 거절한다. 그렇지 않다면 서버 S는 다음을 계산한다..

$$T_u'=h(EID \oplus x) \oplus C_2 \oplus h(x),$$
$$V_u'=h(v, C_2, T_u')$$

만약, V_u=V_u'이라면 서버 S는 사용자 U_i를 인증하고 로그인 요청을 받아들이고, 서버의 타임스탬프 T_s를 이용하여 다음을 계산한다.

$$C_3=h(EID \oplus x) \oplus T_s, \quad V_s=h(v, C_2, C_3, T_s)$$

단계 2 : 서버 S는 사용자 U_i에게 메시지 M_u={V_s, C_3}를 전송한다.

단계 3 : 서버 인증 요청 메시지 M_u={V_s, C_3}를 수신

한 사용자 스마트카드는 T_s'과 V_s'를 계산한다.
$T_s'=C_3 \oplus C_1$, $V_s'=h(v, C_2, C_3, T_s')$
만약, $V_s=V_s'$이라면 사용자 U_i는 성공적으로 서버 S를 인증한다.

4. 스킴 분석

An은 Hsiang-Shih에 의해 제안된 스마트카드를 이용한 사용자 인증 스킴이 패스워드 추측 공격에 취약함을 보였다. 이와 같은 문제점을 해결하기위해 해시함수와 난수에 기반 한 개선된 사용자 인증 스킴을 제안하였다. 그러나 An이 제안한 인증 스킴 역시 오프라인 패스워드 추측공격에 의하여 패스워드가 노출이 된다는 것을 보였다. 인증서버의 비밀키(x)와 타임스탬프(T_u)을 이용하여 오프라인 패스워드 추측공격에 안전한 새로운 스킴에 대한 안전성과 계산 복잡도를 분석한다.

먼저, 개선된 원격 사용자 인증 스킴을 패스워드 추측공격(password guessing attack)과 위조공격(forgery attack)/위장공격(masquerading attack), 재전송공격(replay attack) 등 여러 가지 공격 방법들에 대한 안전성을 분석한다.

4.1 패스워드 추측공격

본 논문에서는 공격자 U_a가 패스워드를 획득할 수 있는 방법은 사용자 U_i의 스마트카드에 저장된 정보를 추출하고 합법적인 사용자 U_i의 메시지를 도청함으로써 오프라인 패스워드 추측 공격을 수행하는 것이다. 즉, 합법적인 사용자 U_i의 인증 요청 메시지 $M_u=\{v, C_2, V_u\}$와 서버 인증 요청 메시지 $M_u=\{V_s, C_3\}$, 그리고 스마트카드에서 불법 추출한 저장 정보 R, h(), b로부터 패스워드 PW_i를 추측하는 것이다. 사용자 U_i의 인증 요청 메시지 $M_u=\{v, C_2, V_u\}$로부터 얻을 수 있는 정보, $C_2= C_1 \oplus h(x) \oplus T_u=h(EID \oplus x) \oplus T_u$로부터 사용자의 패스워드 PW_i를 추출할 수 있는 정보는 없다. 또한, 서버 인증 메시지 $\{M_s, C_3\}$로부터 서버의 임의의 랜덤 nonce N_S와 h(x)를 모르기 때문에 패스워드 PW_i를 추출하는 것은 불가능하다.

4.2 위조공격/위장공격

개선된 인증 스킴에서 공격자가 정당한 사용자로 위장하기 위해서는 아이디와 패스워드를 알아야 한다. 공격자 U_a는 사용자 U_i의 로그인 메시지 $\{v, C_2, V_u\}$를 $\{v, C_2^*, V_u^*\}$로 위조하려 시도할 수 있다. 그러나 이와 같은 위장공격 시도는 검증단계 $T_u'=h(EID \oplus x) \oplus C_2 \oplus h(x)$와 $V_u'=h(v, C_2, T_u')$을 통과 하지 못할 것이다. 그 이유는 공격자 U_a는 유용한 $h(EID \oplus x)$, h(x)의 값을 얻을 수 있는 방법이 없기 때문이다.

4.3 재전송공격

메시지 재전송 공격(replay attack)은 이전 세션의 메시지를 다음 세션에서 재전송하는 방법으로서 불법적인 사용자가 인증을 시도하는 공격이다. 개선된 인증 스킴에서는 매 세션마다 타임스탬프를 사용하기 때문에 공격자는 이전 세션의 정보들로부터 인증 및 검증 정보를 유추할 수 있는 방법이 없다. 또한 서버의 비밀키(x) 추측 공격도 불가능하다. 이것은 공격자가 획득한 정보 즉, 인증 요청 메시지 $M_u=\{v, C_2, V_u\}$와 서버 인증 요청 메시지 $M_u=\{V_s, C_3\}$로부터 서버의 비밀키(x)에 관한 정보를 유추하는 것으로서 해시함수의 일방향성 때문에 불가능하다. 타임스탬프를 이용하여 메시지의 유효성을 검사하고 있기 때문에 시간차를 두고 공격하는 재전송 공격으로부터 안전할 수 있다. 만약, 공격자 U_a가 사용자의 메시지를 저장하고 재전송할 경우 그 메시지는 검증단계에서 검증을 통과할 수 없다.

4.4 기타공격

본 논문에서 제안한 인증 스킴에서는 매 세션마다 새로운 랜덤 값 b을 사용하기 때문에 공격자는 이전 세션의 정보인 로그인 오청 메시지, 인증 요청 메시지와 현재 세션의 정보 $M_u=\{v, C_2, V_u\}$, $M_u=\{V_s, C_3\}$들로부터 인증 및 검증 정보를 유출할 수 있는 방법이 없다. 또한, 공격자는 서버의 비밀키 x은 해시함수의 일방향성 때문에 불가능하고, 비밀키 추측공격도 불가능하다. 그리고 제안한 스킴에서 ID_i 대신 $h(b \oplus ID_i)$를 사용을 하였다. 어느 누구도 사용자의 아이디를 알 수 없다. 심지어 서버도 알 수 없다. 따라서 사용자의 익명성이 보장된다.

4.5 비교 분석

제안한 인증 스킴에 대한 안전성과 계산 복잡도를 An의 인증 스킴과 비교 분석하였다. 본 논문에서는 제안한 인증 스킴의 안전성을 분석하기 위하여 안전성 위협 요소 및 안전성 향상 요소들을 비교 분석하였다. 표 2에서 비교된 바와 같이, An의 인증 스킴은 오프라인 패스워드 추측공격과 위장공격에 취약함을 알 수 있고, 제안한 인증 스킴은 보안 취약점에 강하다는 것을 알 수 있다. 제안한 인증 스킴과 An의 인증 스킴은 exclusive-OR 연산을 사용하기 때문에 계산 복잡도는 매우 작은 계산시간이 요구되기 때문에 그 계산은 무시할 수 있다.

[표 2] 안전성 분석
[Table 2] Analysis of security

스킴	패스워드 추측공격	위장 공격	재전송공격	비밀키 추측공격	익명성
An의 스킴	가능	가능	가능	불가능	가능
제안한 스킴	불가능	불가능	불가능	불가능	불가능

5. 결론

An은 Hsiang-Shih등이 제안한 스마트카드를 이용한 사용자 인증 스킴에 대하여 공격자가 스마트카드에 저장된 정보를 취득함으로써 패스워드 추측공격이 가능하고 이와 함께 합법적인 사용자로 가장할 수 있기 때문에 스마트카드 기반 인증 스킴에서 고려되는 보안 요구 사항을 만족하지 못한다고 했다. 그러나 An이 제안한 사용자 인증 스킴 또한 보안 요구사항에 만족하지 못함을 보이고 이를 개선한 사용자 인증 스킴을 제안하였다. 따라서 본 논문에서 제안한 사용자 인증 스킴은 기존의 스마트 기반 사용자 인증 스킴의 장점을 유지하면서 오프라인 패스워드 추측공격이 불가능하기 때문에 다양한 공격 방법에 대처할 수 있다. 그리고 제안한 인증 스킴은 사용자와 인증 서버가 상대방을 인증할 수 있는 효율적인 상호 인증방식을 제시하였다.

References

[1] L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, Vol.24, No.11, pp. 770-772, 1981.

[2] H.Y. Chien, J .K. Jan, Y. M. Tseng, "An efficient and practical solution to remote authentication using smart card," Computers & Security, 21(4), pp. 372-375, 2002.

[3] S. M. Chen, W. C. Ku, "Weakness and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, 50(1), pp. 204-207, 2004.

[4] E. J. Yoon, E. K. Ryu, K. Y. Yoo, "Further improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, 50(2), pp. 612-614, 2004.

[5] X. Duan, J. W. Liu, 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.

[6] H. C. Hsiang, W. K. Shih, "Weakness and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," Computer Communications 32,pp. 649-652, 2009.

[7] An, "Improvements of the Hsiang-Shih's remote user authentication scheme using smart cards," Journal of the Korea Society of Computer and Information, Vol. 15, No.2, pp. 119-125, 2010.

[8] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," Proceedings of Advances in Cryptology (CRYPTO 99), pp. 388-398, 1999.

[9] T.S, Messerges, E.A, Dabbish, R.H. Sloan, "Examining smart-cards security under the threat of power analysis attacks," IEEE Transactions on Computers, 51(5), pp. 541-552, 2002.

신 승 수(Seung-Soo Shin) **[정회원]**

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야>
암호프로토콜, 네트워크 보안, USN, 스마트 카드,

한 군 희(Kun-Hee Han) **[종신회원]**

- 2008년 8월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
암호프로토콜, 네트워크 보안, 영상처리