Journal of the Korea Academia-Industrial Cooperation Society
Vol. 12, No. 11 pp. 5245-5251, 2011

http://dx.doi.org/10.5762/KAIS.2011.12.11.5245

스마트카드를 이용한 원격 사용자 인증 스킴의 안전성 분석

신승수[1*], 한군희[2], 전제란[3]
[1]동명대학교 정보보호학과, [2]백석대학교 정보통신학부, [3]대전보건대학 의무행정과

Cryptanalysis of a Remote User Authentication scheme using 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**
[3]**Department of Medical Administration, Daejeon Health Science College**

요 약 본 논문에서는 Hu-Niu-Yang이 제안한 스마트카드를 이용한 사용자 인증 스킴에 대하여 Seo등은 공격자가 스마트카드에 저장된 정보를 취득함으로써 패스워드 추측공격(password guessing attack)이 가능하고 이와 함께 합법적인 사용자로 가장할 수 있기 때문에 스마트카드 기반 인증 스킴에서 고려되는 보안 요구 사항을 만족하지 못한다고 했다. 그러나 Seo등의 사용자 인증 스킴 또한 보안 요구사항에 만족하지 않는다. Seo등에 의해 제안된 인증 스킴의 특징을 유지하면서 보안 취약점들을 개선한 스킴을 제안한다. 제안한 사용자 인증 스킴이 Seo등의 인증 스킴보다 상대적으로 안전하고 효율적인 스킴임을 알 수 있다.

Abstract Seo et al. criticizes that Hu-Niu-Yang's certification scheme is not enough to satisfy the security requirements of a smart card-based certification scheme because it has a weakness of password guessing attack as well as gives attackers opportunities to be disguised as legitimate users. However, Seo et al. also has a weakness not satisfying the security requirements. This paper suggests a new scheme that contains the characteristics of certification scheme provided by Seo et al. but compensates weak points. The findings show that the new scheme is more safety and efficient than Seo et al.'s

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

1. 서론

컴퓨터 및 네트워크의 발달로 사용자는 언제 어디서나 다양한 인터넷 서비스를 제공받고자 한다. 또한 분산 컴퓨팅 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.

사용자 인증 프로토콜이란 서비스를 제공하는 서버와 서비스를 이용하려는 사용자간에 서로 상대의 신원을 확인하고 정당한 사용자와 서버라는 것을 상호 검증할 수 있는 프로토콜이다. 패스워드 기반의 스마트카드를 이용한 사용자 인증 스킴의 특징은 원격지에 있는 사용자들이 자신이 기억하고 있는 패스워드와 스마트카드를 이용하여 인증서버로부터 정당한 사용자임을 인증 받을 수 있다.

스마트카드는 마이크로프로세서와 메모리를 내장하고 있어서 카드 내에서 정보의 저장과 처리가 가능한 플라스틱 카드로서 사용자로부터 입력받은 정보를 이용하여 사용자의 로긴 요청 메시지를 생성하여 인증서버로 전송한다. 인증서버와 사용자의 스마트카드는 서로 상대방의 신원 확인과정을 마친 후 상대방이 정당한 통신 상대임

*교신저자 : 신승수(shinss@tu.ac.kr)
접수일 11년 09월 05일 수정일 (1차 11년 09월 26일, 2차 11년 09월 29일, 3차 11년 10월 07일) 게재확정일 11년 11월 10일

을 검증받고 비로소 안전한 통신을 수행한다. 이러한 스킴을 이용하면 원격지에 있는 사용자는 보다 간편하고 안전하게 서버에 접근할 수 있다.

1981년에 Lamport[1]는 암호화 기법을 사용하지 않는 패스워드 기반의 원격 사용자 인증 스킴을 처음으로 제안하였고, 1993년에는 Chang과 Wu[2]은 스마트카드를 갖는 원격 패스워드 인증 스킴을 소개했다. 그 이후 스마트카드 기반 원격 패스워드 인증 스킴은 안전성 또는 효율성을 개선하기 위해 다수 제안되었다. 2002년 Chien[3] 등은 스마트카드를 사용한 효율적인 패스워드 기반 원격 사용자 인증 스킴을 제안하였다. 그러나 Hsu[4] 등은 Chien 등의 스킴은 병렬 세션 공격에 취약함을 지적하였고, Liu[5] 등은 이들 취약점을 방지할 수 있는 개선된 인증 스킴을 제안하였다. 그러나 Hu- Niu-Yang[6]은 Liu등의 스킴 또한 위장서버공격 등 안전성에 취약함을 지적하고, 이를 개선한 사용자 인증 스킴을 제안하였다. 그리고 Seo[7]등은 Hu-Niu-Yang이 제안한 스킴도 공격자가 사용자의 스마트카드에 일시적으로 접근하여 저장된 정보를 획득한 경우에 패스워드 추측 공격(password guessing attack)에 취약함을 지적하였다. 즉, 공격자는 스마트카드에 저장된 정보를 취득함으로써 패스워드 추측 공격이 가능하고 이와 함께 합법적인 사용자로 가장할 수 있다.

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, 도는 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) 또는 (ii)를 수행할 수 없다. (i)의 경우, Kocher 등[9]과 Messerges 등[10]은 모든 스마트카드 안에 저장된 비밀정보는 전력소비를 모니터링 함으로써 추출할 수 있음을 지적하였다. 따라서 카드를 분실하면 카드 안의 모든 정보는 노출된다.

본 논문에서는 Seo등이 제안한 스킴도 패스워드 추측공격과 위장 공격에 취약함을 보이고, 이를 개선한 새로운 스킴을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구로 Seo의 프로토콜을 살펴보고, 문제점을 분석한 후, 3장에서 Seo의 프로토콜을 개선하여 문제점을 해결하고 개선된 프로토콜을 제안한다. 4장에서는 개선된 프로토콜의 안전성과 효율성에 분석하고 5장에서 결론 및 향후 연구에 대해 기술한다.

2. Seo의 인증 스킴 분석

Seo등은 Hu-Niu-Yang의 스킴은 패스워드 기반 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 만족하지 않는다고 보였다. 즉, 공격자가 사용자의 스마트카드에 불법적적으로 접근할 수 있다면 스마트카드에 저장된 정보를 추출함으로서 패스워드 추측 공격과 함께 합법적인 시스템 사용자로 가정할 수 있다. 그러므로 Hu-Niu-Yang의 스킴은 스마트카드 기반 인증 시스템이 갖춰야 하는 안전성 요구사항을 만족하지 못한다. Seo등 개선된 인증 스킴을 제안하였으나, 또한 패스워드 추측공격, 위조 및 위장공격 등에 대한 안전성 요구사항을 만족하지 않는다.

본 논문에서 관련 연구 및 제안한 스킴에 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
N_u, N_S	사용자 및 인증서버에 의해 생성된 랜덤 nonce
h()	안전한 일방향 해시함수
‖	연접
⊕	XOR 비트 연산자
T_R	사용자가 서버에 등록할 때의 타임스탬프

2.1 Seo의 스킴

Seo등은 Hu-Niu-Yang가 제안한 인증 스킴을 개선하고, 패스워드 추측공격과 위장공격에 안전한 새로운 스킴을 제안하였다.

<등록단계>

(1) U_i는 랜덤 값 b와 패스워드 PW_i를 선택하고, 해시값 $h(b \oplus PW_i)$를 계산한다.

(2) U_i는 S에게 ID_i, $h(b \oplus PW_i)$를 전송한다.

(3) 만약, U_i가 초기등록이면, S는 U_i를 위한 계정 데이

터베이스를 생성하고, 초기등록이 아니면, S는 데이터베이스의 항목을 변경한다. 그리고 S는 다음 식을 계산을 수행한다.

$X_S=h(ID_T \oplus_X)$, $R=X_S \oplus (b \oplus PW_i)$

여기서, $ID_T=(ID_i \| T_R)$이다.

(4) S는 U_i에게 R, ID_i 그리고 h()이 저장된 스마트카드를 발급한다.

(5) U_i는 b를 스마트카드에 저장한다.

<로그인단계>

(1) U_i는 스마트카드를 스마트카드 리더에 넣고 ID_i와 PW_i를 입력한다.

(2) U_i의 스마트카드는 다음 수식을 계산하여 수행한다.

$C_1=R \oplus (b \oplus PW_i)$, $M_i=C_1 \oplus N_u$,

$C_2=h(ID_i \oplus M_i \oplus h(N_i))$

여기서, N_u는 스마트카드에 의해 선택된 랜덤 nonce이다.

(3) 사용자 U_i는 서버 S에게 인증 요청 메시지 $\{ID_i, M_i, C_2\}$를 송신한다.

<인증단계>

(1) 만약, ID_i가 유효하면 사용자 인증을 위해 다음을 식을 계산한다. 그렇지 않다면 S는 U_i의 로그인 요청을 거절한다.

$$N_u'=M_i \oplus h(ID_T \oplus_X),$$
$$C_2'=h(ID_i \oplus M_i \oplus h(N_u'))$$

만약, $C_2'=C_2$이면 S는 U_i를 인증하고 로그인 요청을 받아들인다.

(2) 그런 다음 S는 랜덤 nonce N_S를 생성하여 이를 이용하여 다음 식을 계산한다.

$$M_S=h(ID_T \oplus_X) \oplus N_S,$$
$$C_3=h(ID_i \oplus M_i \oplus M_S \oplus h(N_S))$$

(3) S는 U_i에게 인증요청 메시지 $\{M_S, C_3\}$를 전송한다.

(4) 서버 인증요청 메시지 $\{M_S, C_3\}$를 수신한 사용자 U_i의 스마트카드는 다음 식을 계산한다.

$$N_S'=C_1 \oplus M_S,$$
$$C_3'=h(ID_i \oplus M_i \oplus M_S \oplus h(N_S'))$$

만약, $C_3'=C_3$이면 U_i는 S를 성공적으로 인증한다.

<패스워드 변경 단계>

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

(2) 스마트카드는 인증서버와 상호작용에 의해 PW_i의 유용성을 확인하고, 성공하면, $R(=X_S \oplus (b \oplus PW_i))$을 $R \oplus (b \oplus PW_{i_new}))$으로 변경한다.

2.2 Seo의 스킴 분석

Seo등은 Hu-Niu-Yang의 인증 스킴에 대해 개선된 스킴을 제안하였다. 그러나, Seo등 스킴도 패스워드 추측공격 및 위장공격에 취약함에 대해 분석한다.

Kocher[9]와 Messerges[10]의 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 패스워드 추측공격을 수행할 수 있다.

2.2.1 오프라인 패스워드 추측공격

Seo등이 제안한 스킴은 오프라인 패스워드 추측공격에 대한 안전성에 문제가 있음을 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 다음과 같은 과정으로 사용자 U_i의 패스워드를 알아낼 수 있다.

1 : 정당한 사용자 U_i는 로그인 요청 메시지 $\{ID_i, M_i C_2\}$을 생성하여 인증서버 S로 전송한다.

2 : 이때 공격자 U_a는 정당한 사용자 U_i의 로그인 요청 메시지를 가로채서 C_2과 M_i를 획득한다.

3 : 공격자 U_a는 획득한 정보를 이용하여 오프라인 패스워드추측 공격을 다음과 같이 수행한다.

(1) 공격자 U_a는 정당한 사용자 U_i의 패스워드 PW_i'로 추측한다.

(2) 공격자 U_a는 스마트카드로부터 추출한 정보 R, PW_i'로부터 $C_1'=R \oplus h(b \oplus PW_i')$를 계산한다.

(3) 다음은 획득한 M_i를 이용하여 N_u'을 얻는다.

$$M_i \oplus C_1' = N_u'$$

(4) C_1'과 N_u'를 이용하여 $C_2'=h(ID_i \oplus M_i \oplus h(N_u'))$를 계산한다.

(5) 계산한 C_2'와 불법 획득한 C_2가 동일한 값인지를 확인한다.

(6) 공격자 U_a는 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.

따라서, Seo등이 제안한 스킴도 오프라인 패스워드 추측공격에 대한 안전성에 문제가 있다.

2.2.2 위장 공격

Seo등이 제안한 스킴에 대하여 위장공격에 취약함에 대해 분석한다. 먼저 서버 위장공격과 사용자 위장공격에 대하여 분석한다. 공격자 U_a는 로그인 단계에서 사용자 U_i가 서버에 전송하는 메시지 $\{ID_i, C_2, M_i\}$를 가로챌 수 있다. 공격자 U_a는 서버로 보내는 메시 $\{ID_i, C_2, M_i\}$를 가로채서 스마트카드에 의해 선택된 랜덤 nonce N_u 대신 새로운 난수 N_u'를 사용하여 다음을 계산한다.

$$M_i'=h(ID_T \oplus x) \oplus N_u',$$
$$C_2'=h(ID_i \oplus M_i' \oplus h(N_u'))$$

그리고, 공격자 U_a는 로그인 단계에서 가로챈 메시지 $\{ID_i, C_2, M_i\}$를 $\{ID_i, C_2', M_i'\}$로 수정하여 서버에 전송한다. 서버는 수신된 메시지 $\{ID_i, C_2', M_i'\}$로부터 ID_i의 유효성 검사를 하고 사용자 인증을 다음과 같이 한다.

$$N_u''=M_i' \oplus h(ID_T \oplus x),$$
$$C_2''=h(ID_i \oplus M_i' \oplus h(N_u''))$$

만약, $C_2''=C_2'$이면 서버는 S는 사용자 U_i를 인증하고 로그인 요청을 받아들인다. 그런 다음 서버 S는 랜덤 nonce N_s를 생성하고 이를 이용하여 다음을 계산한다.

$$M_s=h(ID_T \oplus x) \oplus N_s,$$
$$C_3=h(ID_i \oplus M_i \oplus M_s \oplus h(N_s))$$

서버 S는 사용자 U_i에게 인증요청 메시지 $\{C_3, M_s\}$를 전송한다.

이때, 공격자 U_a는 사용자 U_i에게 보내는 메시지를 가로채어 서버 S에 의해 선택된 랜덤 nonce N_s 대신 새로운 난수 N_s'를 사용하여 다음을 계산하여 사용자U_i에게 $\{C_3', M_s'\}$를 전송한다.

$$M_s'=h(ID_T \oplus x) \oplus N_s',$$
$$C_3'=h(ID_i \oplus M_i \oplus M_s \oplus h(N_s'))$$

서버 인증 요청 메시지 $\{C_3', M_s'\}$를 수신한 사용자 U_i의 스마트카드는 다음을 계산한다,

$$N_S''=C_1 \oplus M_S',$$
$$C_3''=h(ID_i \oplus M_i \oplus M_S' \oplus h(N_S'))$$

만약, $C_3''=C_3'$이면 사용자 U_i는 서버 S를 성공적으로 인증한다. 그리고, 이 스킴은 인증단계에서 사용자의 패스워드가 올바른지 아닌지를 판단할 수 있는 것을 제공하지 못한다.

따라서, Seo등이 제안한 인증 스킴은 오프라인 패스워드 추측공격과 위장공격에 취약하다. 이를 개선한 스킴을 제안하고자 한다.

3. 제안 인증 스킴

본 장에서는 Seo등에 의해 제안된 인증 스킴의 특징을 유지하면서 보안 취약점들을 개선한 스킴을 제안한다. 개선된 인증 스킴은 등록단계, 로그인 단계, 인증 단계, 그리고 패스워드 변경 단계로 구성된다.

3.1 등록 단계

이 단계는 사용자 U_i가 원격 시스템인 서버 S에 등록할 때 수행된다.

단계 1 : 사용자 U_i는 랜덤 값 b와 패스워드 PW_i를 선택하고, 해시값 $h(b \oplus PW_i)$, $h(b \oplus ID_i)$을 계산한다.

단계 2 : 사용자 U_i는 서버 S에게 $h(b \oplus PW_i)$, $h(b \oplus ID_i)$을 안전한 채널로 전송한다.

단계 3 : 만약, 사용자 U_i가 초기등록이면, 서버 S는 사용자 U_i를 위한 계정 데이터베이스를 생성하고, 초기등록이 아니면, 서버 S는 데이터베이스 항목을 변경한다. 그리고 서버 S는 다음을 계산한다.

$$R=h(b \oplus ID_i) \oplus h(x), \quad M=R \oplus h(b \oplus PW_i)$$

단계 4 : 서버 S는 사용자 U_i에게 M, h()이 저장된 스마트카드를 발급한다.

단계 5 : 사용자 U_i는 b를 스마트카드에 저장한다.

3.2 로그인 단계

이 단계는 사용자 U_i가 서버 S에게 로그인을 요청할 때마다 실행된다.

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

단계 2 : 사용자 U_i의 스마트카드는 다음을 계산한다.

$$C_1=M \oplus h(b \oplus PW_i),$$
$$M_i=C_1 \oplus h(x) \oplus N_u,$$
$$C_2=h(M_i \oplus h(x) \oplus h(N_u))$$

여기서, N_u는 스마트카드에 의해 선택된 랜덤 nonce이다.

단계 3 : 사용자 U_i는 서버 S에게 인증 요청 메시지 $\{R, M_i, C_2\}$를 송신한다.

3.3 인증 단계

원격시스템 S는 정당한 사용자 U_i로부터 인증 요청 메시시 $\{R, M_i, C_2\}$를 수신한 후에 다음을 수행한다.

단계 1 : 만약 ID_i가 유효하다면 사용자 인증을 위해 다음 식을 계산한다. 그렇지 않다면 서버 S는 사용자 U_i의 로그인 요청을 거절한다.

$$N_u'=M_i \oplus h(ID_i \oplus b),$$
$$C_2'=h(M_i \oplus h(x) \oplus h(N_u'))$$

만약, $C_2'=C_2$이면 서버 S는 사용자 U_i를 인증하고 로그인 요청을 받아들인다.

단계 2 : 그런 다음 서버 S는 랜덤 nonce N_S를 생성하여 이를 이용하여 다음 식을 계산한다.

$$M_S=h(ID_i \oplus b) \oplus h(x) \oplus N_S,$$
$$C_3=h(M_i \oplus M_S \oplus h(N_S))$$

단계 3 : 서버 S는 사용자 U_i에게 인증 요청 메시지 $\{M_S, C_3\}$를 전송한다.

단계 4 : 서버 인증 요청 메시지 $\{M_S, C_3\}$를 수신한 U_i의 스마트카드는 다음 식을 계산한다.

$$N_S'=C_1 \oplus M_S,$$
$$C_3'=h(M_i \oplus M_S \oplus h(N_S'))$$

만약, $C_3'=C_3$이면 사용자 U_i는 서버 S를 성공적으로 인증한다.

3.4 패스워드 변경 단계

(1) 사용자 U_i는 스마트카드를 카드 리더에 넣고 아이디 ID_i와 패스워드 PW_i를 입력하고 패스워드 변경을 요청한다.

(2) 스마트카드는 인증서버 S와 상호작용에 의해 PW_i의 유효성을 확인하고, 성공하면, $M(=R \oplus h(b \oplus PW_i))$을 $R \oplus (b \oplus PW_{i_new}))$으로 변경한다.

4. 개선된 스킴 분석

본 장에서는 개선된 스킴에 대한 스마트카드 기반 인증 시스템이 갖춰야 하는 안전성 요구사항에 대하여 분석한다. 개선된 인증 스킴에서 패스워드 추측공격(password guessing attack), 위장공격(impersonation attack) 등에 하기 위해 획득 가능한 정보, 즉 합법적인 사용자 U_i의 스마트카드 정보들, 사용자 인증 요청 메시지와 서버 인증 메시지들로부터 안전성을 분석한다.

1) 패스워드 추측공격

패스워드 추측공격은 온라인과 오프라인 패스워드 추측공격으로 나눌 수 있다. 온라인 패스워드 추측공격은 인증 실패 횟수를 계산함으로써 쉽게 탐지되고 조치될 수 있으므로, 본 논문에서는 오프라인 패스워드 추측공격에 대해서만 고려한다.

본 논문에서는 공격자 U_a가 패스워드를 획득할 수 있는 방법은 사용자 U_i의 스마트카드에 저장된 정보를 추출하고 합법적인 사용자 U_i의 메시지를 도청함으로써 오프라인 추측공격을 수행하는 것이다. 즉, 합법적인 사용자 U_i의 인증 요청 메시지 $\{R, M_i, C_2\}$와 서버 인증 요청 메시지 $\{M_S, C_3\}$ 그리고 스마트카드에서 불법 추출한 저장 정보 R, h(), b로부터 패스워드 PW_i를 추측하는 것이다. 사용자 U_i의 인증 요청 메시지 $\{R, M_i, C_2\}$로부터 얻을 수 있는 정보 $M_i=C_1 \oplus h(x) \oplus N_u = h(ID_i \oplus b) \oplus N_u$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.

2) 위장공격

합법적인 사용자 A와 B가 서버로부터 인증을 받은 올바른 사용자라고 가정하자. 위장공격(Impersonation attack)이란 공격자가 자신이 B인 것처럼 속이고 A와 프로토콜을 진행하는 것을 말한다.

본 논문에서는 서버 위장공격과 사용자 위장공격에 대하여 분석한다. 공격자 U_a는 로그인 단계에서 사용자 U_i가 서버에 전송하는 메시지 $\{R, M_i, C_2\}$를 가로챌 수 있다. 공격자 U_a는 서버 S로 보내는 메시 $\{R, M_i, C_2\}$를 가로채서 스마트카드에 의해 선택된 랜덤 nonce N_u 대신 새로운 난수 N_u'를 사용하여 다음을 계산한다.

$$N_u'=M_i \oplus h(ID_i \oplus b),$$
$$C_2'=h(M_i \oplus h(x) \oplus h(N_u'))$$

즉, 공격자 U_a는 로그인 단계에서 가로챈 메시지 $\{R, M_i, C_2\}$를 $\{R, M_i, C_2'\}$로 수정하여 서버 S에 전송한다. 그러나 공격자 U_a는 로그인 단계에서 가로챈 메시지 $\{R, M_i, C_2\}$로부터 랜덤 nonce N_u와 h(x)를 얻을 수 없기 때문에 서버 S에 성공적으로 로그인을 할 수 없다. 다음은 서버 위장 공격에 대하여 분석한다. 서버 S는 랜덤 nonce N_s를 생성하고 이를 이용하여 다음을 계산한다.

$$M_s=h(ID_T \oplus x) \oplus N_s,$$
$$C_3=h(ID_i \oplus M_i \oplus M_s \oplus h(N_s))$$

서버 S는 사용자 U_i에게 인증요청 메시지 $\{C_3, M_s\}$를 전송한다.

이때, 공격자 U_a는 사용자 U_i에게 보내는 메시지 $\{C_3, M_s\}$를 가로채어 서버에 의해 선택된 랜덤 nonce N_s 대신 새로운 난수 N_s'를 사용하여 다음을 계산하려 한다.

$$N_S'=C_1 \oplus M_S,$$
$$C_3'=h(M_i \oplus M_S \oplus h(N_S'))$$

그러나 공격자 U_a는 $h(ID_i \oplus b)$, h(x), N_S 등의 정보를

얻을 수 없기 때문에 인증요청 메시지 $\{C_3, M_s\}$로부터 $\{C_3', M_s'\}$를 전송하여 보낸 정보는 $C_3''\neq C_3'$이기 때문에 인증에 성공하기 못한다.

제안한 인증 스킴도 등록단계, 로그인단계, 인증단계 모두가 hash function과 exclusive-OR 연산을 기반으로 구성 되어 있다. 따라서 exclusive-OR 연산은 매우 작은 계산을 요구하기 때문에 일반적으로 그 계산은 무시한다. 따라서 Seo등이 제안한 스킴과 본 논문에서 제안한 스킴과의 계산복잡도 측면에서는 별 차이가 없다.

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

스킴	패스워드 추측공격	위장공격	재전송공격
Seo의 스킴	가능	가능	가능
제안한 스킴	불가능	불가능	불가능

5. 결론

본 논문에서는 Hu-Niu-Yang이 제안한 스마트카드를 이용한 사용자 인증 스킴에 대하여 Seo등은 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 Seo등의 사용자 인증 스킴 또한 보안 요구사항에 만족하지 않는다. 이를 개선한 사용자 인증 스킴을 제안하였다. 개선된 사용자 인증 스킴은 공격자가 사용자의 스마트카드에 저장된 정보를 추출한 후 그것을 이용하여 사용자의 패스워드를 알아내려 하여도 알 수가 없다. 즉, 제안한 스킴은 패스워드 추측공격, 위장공격에도 불가능하다. 그리고 사용자와 서버가 상대방을 인증을 할 수 있는 효율적인 상호 인증방식을 제시하였다. 이러한 스킴은 기존의 스마트카드 기반 사용자 인증 스킴에 효율적으로 많이 이용될 수 있을 것으로 기대된다.

References

[1] L. Lamport, "Password authentication with insecure communication," Communication of the ACM, 24(11), pp. 770-772, 1981.

[2] C.C Chang, T.C. Wu, "Remote password authentication with smart cards," IEEE Proceedings-E, 138(3), pp. 165-168, 1991.

[3] 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.

[4] C.L. Hsu, "Security of two remote user authentication schemes using smart card," IEEE Transactions on Consumer Electronics, 49(4), pp. 1196-1198, 2003.

[5] J.Q. Kiu, J. Sun, T.H. Li, "An enhanced remote login authentication with smart card," Proceedings of IEEE Workshop on Signal Proceeding Systems Design and telecommunications, vol. 14, pp. 91-94, 2005.

[6] L.L. Hu, X.X. Niu, Y.X. Yang, "Weakness and improvements of a remote user authentication scheme using smart cards," The journal of China univ. of posts and telecommunications, vol. 14, pp. 91-94, 2007.

[7] J. M. Seo, H. Y. An, "Security Improvements on the Remote User Authentication Scheme Using Smart Cards", Journal of the Korea Society of Computer and Information, Vol. 15, No.3, pp. 91-97, 2010. 3.

[8] J. Xu, W.T Zhu, 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, B. Jun, "Differential power analysis," Proceedings of Advances in Cryptology (CRYPTO 99), pp. 388-398, 1999.

[10] 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

전 제 란(Chun Je Ran) **[정회원]**

- 2005년 8월 : 청주대학교 경영학과경영학석사
- 2008년 8월 : 청주대학교 경영학과경영학박사
- 1997년 ~ 2008.12월 : (의) 정산의료재단 효성병원 경영관리원장
- 2010년 3월 ~ : 대전보건대학교 의무행정과 교수

<관심분야>
병원경영성과평가, 보건행정, 병원CRM, 의료관광, 병원정보시스템