韓國컴퓨터情報學會 論文誌
第15卷 第3號, 2010. 3.

2010-15-3-3-5

스마트카드를 사용한 원격 사용자 인증 스킴의 시큐리티 개선에 관한 연구

서 정 만*, 안 영 화**

Security Improvements on the Remote User Authentication Scheme Using Smart Cards

Seo Jeong Man*, An Young Hwa**

요 약

최근 Hu-Niu-Yang은 Liu 등의 스킴을 개선한 사용자 인증 스킴을 제안하였다. 그러나 Hu-Niu-Yang의 스킴은 패스워드 기반 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 만족하지 못하고 있다. 본 논문에서는, 공격자가 사용자의 스마트카드를 훔치거나 일시적으로 접근할 수 있는 경우에 Hu-Niu-Yang의 스킴은 off-line 패스워드 추측공격에 취약하다는 것을 증명하였다. 또한 이와 같은 안전성 취약점들을 해결한 개선된 사용자 인증 스킴을 새로이 제안하였다. 제안된 사용자 인증 스킴은 패스워드 추측공격, 위조 및 위장공격, 그리고 재생공격 등을 방지한 안전한 인증 스킴임을 알 수 있었고, 이와 같은 공격들을 방지하기 위하여 hash 및 exclusive-OR 연산이 상대적으로 Hu-Niu-Yang의 스킴보다 다수 필요함을 알 수 있었다.

Abstract

Recently Hu-Niu-Yang proposed the user authentication scheme to improve Liu et al's scheme. But the Hu-Niu-Yang's scheme has not been satisfied security requirements considering in the user authentication scheme using the password based smart card. In this paper, we proved that Hu-Niu-Yang's scheme is vulnerable to the off-line password guessing attack in case that the attacker steals the user's smart card and extracts the information in the smart card. Also, the improved user authentication scheme solving the security vulnerability was introduced, thus preventing the attacks, such as password guessing attack, forgery attack impersonation attack, and replay attack. For preventing those attacks, the our proposed scheme need more hash functions and exclusive-OR operations than Hu-Niu-Yang's scheme.

▸ Keyword : 사용자 인증(User Authentication), 스마트카드(Smart Card), 패스워드 추측공격(Password Guessing Attack)

• 제1저자 : 서정만 교신저자 : 안영화
• 투고일 : 2010. 03. 05, 심사일 : 2010. 03. 11, 게재확정일 : 2010. 03. 16.
* 국립한국재활복지대학 컴퓨터게임개발과 교수 **강남대학교 컴퓨터미디어정보공학부 교수

Ⅰ. 서 론

컴퓨터 네트워크 기술의 발달과 함께, e-commerce 및 m-commerce에서의 사용자 인증은 중요한 자원에 액세스하기 위해 필수적인 요인이다. 사용자 인증 프로토콜이란 서비스를 제공하는 서버와 이를 이용하려는 사용자 간에 서로 상대방의 신원을 확인하고 정당한 사용자와 서버라는 검증을 수행하는 프로토콜이다. 이와 같은 사용자 인증 프로토콜에 의해 사용자는 사전에 서비스를 제공하는 서버에 자신의 신원을 확인받을 수 있는 정보를 등록하고, 정당한 사용자임을 검증받고 서비스를 제공 받고 싶을 때 언제 어디서나 서버가 제공하는 서비스를 이용할 수 있다.

일반적으로 스마트카드 기반 패스워드 인증 스킴은 인증서버의 오버헤드는 줄이고 사용자는 오직 자신의 패스워드만을 기억할 필요가 있다. 로그인 메시지를 생성하고 전송하는 것 이외에도 스마트카드는 또한 상호 인증을 제공한다. 본 논문에서는 스마트카드 기반 사용자 인증 스킴의 안전성을 평가하기 위해 공격자는 다음과 같은 능력을 갖고 있다고 가정한다[1].

- 공격자는 로그인 단계 및 인증 단계에서 서버와 사용자 간에 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[2]과 Messerges 등[3]은 모든 스마트카드 안에 저장된 비밀정보는 전력소비를 모니터링함으로서 추출할 수 있음을 지적하였다. 따라서 일단 카드를 분실하면 카드 안의 모든 정보는 노출된다.

(iii)의 경우, 사용자 스마트카드와 자신의 패스워드를 도난당한다면 공격자가 사용자로 위장하는 것을 방지할 수 없다. 따라서 본 논문에서는 스마트카드는 일시적으로 도난당했으나 패스워드는 공격자에게 노출되지 않은 경우에 패스워드 인증 스킴에 대해 논의하고자 한다.

1981년에 Lamport는 암호화 기법을 사용하지 않은 패스워드 기반의 원격 사용자 인증 스킴을 처음으로 제안하였고[4], 1993년에는 Chang 등은 스마트카드를 갖는 리모트 패스워드 인증 스킴을 소개했다[5]. 그 이후 스마트카드 기반 리모트 패스워드 인증 스킴은 안전성, 또는 효율을 개선하기 위해 다수 제안되었다[1][4-17]. 2002년에 Chien 등은 스마트카를 사용한 효율적인 패스워드 기반 리모트 사용자 인증 스킴을 제안하였다[6]. 그러나 Hsu 등은 Chien 등의 스킴은 병렬 세션 공격에 취약함을 지적하였고[7], Liu 등은 이들 취약점을 방지할 수 있는 개선된 인증 스킴을 제안하였다[8]. 그러나 Hu-Niu-Yang은 Liu 등의 스킴 또한 위장 서버 공격 등 안전성에 취약함을 지적하였고, 이를 개선한 사용자 인증 스킴을 제안하였다[9].

본 논문에서는 Hu-Niu-Yang이 제안한 스킴도 공격자가 사용자의 스마트카드에 일시적으로 접근하여 저장된 정보를 획득한 경우에 패스워드 추측 공격(password guessing attack)에 취약함을 지적하였다. 다시 말하면, 공격자는 스마트카드에 저장된 정보를 취득함으로서 패스워드 추측공격이 가능하고 이와 함께 합법적인 사용자로 가장할 수 있다. 따라서 Hu-Niu-Yang의 스킴은 스마트카드 기반 인증 스킴에서 고려되는 보안 요구사항을 만족하지 못한다.

또한 본 논문에서는 Hu-Niu-Yang의 스킴 특성을 유지하면서, 위와 같은 안전성 취약점들을 개선한 스마트카드 기반 인증 시스템을 새로이 제안하였다.

본 논문의 구성은 다음과 같다. 제Ⅱ장에서 Hu-Niu-Yang의 스마트카드를 이용한 사용자 인증 스킴을 기술하고, 그 안전성을 분석하였다. 제Ⅲ장과 Ⅳ장에서는 개선된 인증 스킴을 새로이 제안하고, 안전성을 분석하였다. 그리고 Ⅴ장에서 결론을 맺는다.

Ⅱ. Hu-Niu-Yang의 인증 스킴 및 안전성 분석

중요 정보시스템의 접근에 있어 사용자 인증과정은 반드시 필요하다. 인증과정에는 여러 가지 방법과 절차가 있지만, 현재는 단순한 암호와 아이디 만을 사용한 1단계적인 인증을 대다수 사용하고 있으며 1단계 인증보다 강력한 인증이 필요한 경우에만 OTP 및 인증서등을 이용한 2단계적인 인증을 사용하고 있다[17]. 또한 생체인증과 같은 3단계 인증을 사용하는 경우도 있으나 오인식율과 오거부율이 발생하여 중요정보 시스템의 접근에 사용하기보다는 중요 정보시스템이 보관되어 있는 장소 등과 같이 물리적 보안이 필요한 곳에서만 제한적으로 사용하고 있다.

본 논문에서 사용자의 인증에 사용될 표기법에 대하여 다음과 같이 정의한다.

Ui : 사용자 i

IDi : 사용자 i의 아이디

Pi : 사용자 i의 패스워드
S : 인증 서버
x : 인증 서버의 비밀키
Ni, Ns : 사용자 및 인증 서버에 의해 생성된 랜덤 nonce
h() : 안전한 일방향 해쉬 함수
‖ : 연접

2.1 Hu-Niu-Yang의 인증 스킴

본 장에서는 Hu-Niu-Yang이 제안한 스마트카드를 이용한 사용자 인증 스킴[9]을 간략히 기술한다. 이 스킴은 등록 단계, 로그인 단계, 그리고 인증 단계로 구성된다.

2.1.1 등록 단계

이 단계는 사용자 Ui가 인증 서버 S에 등록할 때 수행된다.

(1) U_i는 랜덤 값 b와 패스워드 P_i를 선택하고, 해쉬값 $h(b \oplus P_i)$를 계산한다.

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

(3) 만약 U_i가 초기 등록이면, S는 U_i를 위한 계정 데이터베이스를 생성하고, 초기 등록이 아니면, S는 데이터베이스의 항목을 변경한다. 그리고 S는 다음 식(2.1) 계산을 수행한다.

$$R=h(ID_T \oplus x) \oplus h(b \oplus P_i) \cdots\cdots (2.1)$$

여기서, $ID_T=(ID_i \| T_R)$이다.

(4) S는 U_i에게 R, ID_i, e 그리고 $h()$이 저장된 스마트카드를 발급한다. 여기서 e는 서버에 의해 생성된 랜덤 수이다.

(5) U_i는 b와 P_i를 스마트카드에 입력하고, $K=h(P_i)$을 계산한 후 b와 K를 스마트카드에 저장한다.

2.1.2 로그인 단계

이 단계는 사용자 Ui가 인증 서버 S에게 로그인을 요청할 때마다 수행된다.

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

(2) U_i의 스마트카드는 ID_i의 유효성을 확인하고 $h(P_i)$가 저장된 K값과 같은 지를 검증한 후에 다음 식(2.2) 계산을 수행한다.

$$C_1=R \oplus h(b \oplus P_i)$$
$$M=h(e \| N_u)$$
$$C_2=h(C_1 \oplus M \oplus e) \cdots\cdots (2.2)$$

(3) U_i는 S에게 $\{ID_i, C_2, M\}$을 송신한다.

2.1.3 인증 단계

이 단계는 인증 서버 S가 사용자 Ui의 로그인 요청을 수신할 때마다 수행된다.

(1) 만약 ID_i 가 유효하지 않으면 S는 U_i의 로그인 요청을 거절한다. 그렇지 않다면 S는 $h(e \| N_s)$를 계산한다. 만약 계산 결과가 수신된 M값과 같으면 S는 다음 단계를 수행하고, 다르면 S와 U_i는 N_u를 N_s로 동기시키는 과정을 수행한다.

(2) S는 $h(h(ID_T \oplus x) \oplus M \oplus e)$를 계산한다. 만약에 계산된 결과 값이 C_2와 같으면, S는 U_i의 로그인 요청을 받아들이고 $N_s=N_s+1$로 세팅한다. 그리고 나서 인증 서버 S는 다음 식(2.3)을 계산하고 사용자 U_i에게 전송한다.

$$C_3=h(h(ID_T \oplus x) \oplus h(e \| N_s)) \cdots\cdots (2.3)$$

(3) U_i의 스마트카드는 $h(C_1 \oplus h(e \| (N_u+1)))$를 계산한 후 수신된 C_3과 비교한다. 만약 값이 같다면 U_i는 성공적으로 서버 S를 인증하고 $N_u=N_u+1$로 세팅한다.

2.2 안전성 분석

본 장에서는 Hu-Niu-Yang의 인증 스킴에 대해서 패스워드 추측공격(password guessing attack) 측면에서 안전성을 분석한다. 이 공격을 수행하기 위해 공격자 Ua는 사용자 Ui의 스마트카드를 훔치거나 일시적으로 접근하여 그 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정한다. 따라서 사용자 Ui의 스마트카드로부터 R, e, b, K를 추출한 공격자 Ua는 사용자 Ui의 패스워드를 알아낼 수 있다. 그 수행과정은 다음과 같다.

단계 1. 인증서버에 로그인하기 위한 사용자 U_i는 로그인 요청 메시지 $\{ID_i, C_2, M\}$을 생성하여 인증서버로 전송한다.

단계 2. 이때 공격자 U_a는 사용자 U_i의 로그인 요청

메시지를 가로채서 M과 C_2를 획득한다.

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

(1) 공격자 U_a는 사용자 U_i의 패스워드를 P_i'로 추측한다.

(2) $C_2'=h(C_1'\oplus M\oplus e)=h((R\oplus h(b\oplus P_i'))\oplus M\oplus e)$를 계산한다.

(3) 계산한 C_2'와 불법 획득한 C_2가 동일한 값인 지를 확인한다.

(4) 공격자는 추측한 P_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 P_i'는 사용자 U_i의 패스워드이다.

또한, 공격자 U_a는 불법 획득한 K로부터 간단히 사용자 U_i의 패스워드를 알아낼 수 있다. 즉, $K=h(P_i')$로부터 단계별 패스워드추측 공격을 수행하면 용이하게 패스워드를 찾아낼 수 있다.

이와 같이 Hu-Niu-Yang이 제안한 스마트카드를 이용한 사용자 인증 스킴은 오프라인 패스워드 추측 공격 방식을 이용하면 사용자의 패스워드를 찾아 낼 수 있기 때문에 안전성에 취약함을 알 수 있다.

III. 제안한 인증 스킴

본 장에서는 hash 함수와 random nonce를 이용하여 Hu-Niu-Yang의 인증 스킴[9]을 개선하였다. 개선된 인증 스킴은 Hu-Niu-Yang의 인증 스킴의 특성을 유지하면서 다양한 안정성 취약점들을 해결할 수 있다. 제안한 인증 스킴은 그림 1과 같이 등록 단계, 로그인 단계, 인증 단계, 그리고 패스워드 변경 단계로 구성된다.

3.1 등록 단계

이 단계는 사용자 Ui가 서버 S에 등록할 때 수행된다. 여기서 TR은 Ui가 S에 등록할 때의 타임스탬프이다.

(1) U_i는 랜덤 값 b와 패스워드 P_i를 선택하고, 해쉬값 $h(b\oplus P_i)$를 계산한다.

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

(3) 만약 U_i가 초기 등록이면, S는 U_i를 위한 계정 데이터베이스를 생성하고, 초기 등록이 아니면, S는 데이터베이스의 항목을 변경한다. 그리고 S는 다음 식(3.1)계산을 수행한다.

$$X_s=h(ID_T\oplus x)$$
$$R=X_s\oplus h(b\oplus P_i) \cdots\cdots (3.1)$$

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.

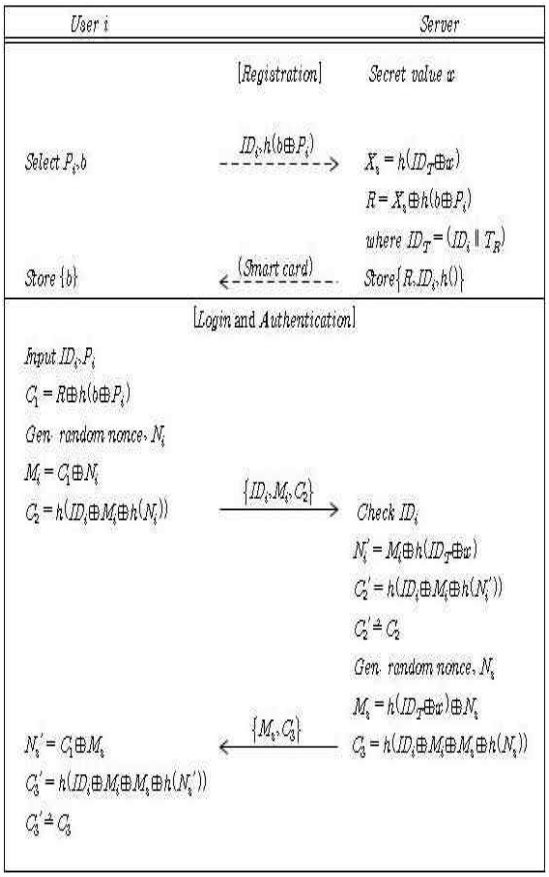

그림 1. 제안한 인증 스킴
Fig 1. The our proposed scheme

3.2 로그인 단계

이 단계는 사용자 U_i가 인증 서버 S에게 로그인을 요청할 때마다 수행된다.

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

(2) U_i의 스마트카드는 다음 식(3.2) 계산을 수행한다.

$$C_1=R\oplus h(b\oplus P_i)$$
$$M_i=C_1\oplus N_i$$
$$C_2=h(ID_i\oplus M_i\oplus h(N_i)) \cdots\cdots (3.2)$$

여기서, N_i는 스마트카드에 의해 선택된 랜덤 nonce이다.

(3) U_i는 S에게 인증요청 메시지 $\{ID_i, M_i, C_2\}$를 송신한다.

3.3 인증 단계

원격 시스템 S는 인증요청 메시지 $\{ID_i, M_i, C_2\}$를 수신한 후에 다음을 수행한다.

(1) 만약 ID_i가 유효하면 사용자 인증을 위해 식(4.3)을 계산한다. 그렇지 않다면 S는 U_i의 로그인 요청을 거절한다.

$$N_i'=M_i\oplus h(ID_T\oplus x)$$
$$C_2'=h(ID_i\oplus M_i\oplus h(N_i')) \cdots\cdots (3.3)$$

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

(2) 그런 다음 S는 랜덤 nonce N_s를 생성하고 이를 이용하여 식(4.4)를 계산한다.

$$M_s=h(ID_T\oplus x)\oplus N_s$$
$$C_3=h(ID_i\oplus M_i\oplus M_s\oplus h(N_s)) \cdots\cdots (3.4)$$

(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 식(3.5)를 계산한다.

$$N_s'=C_1\oplus M_s$$
$$C_3'=h(ID_i\oplus M_i\oplus M_s\oplus h(N_s')) \cdots\cdots (3.5)$$

만약 $C_s'=C_s$이면 U_i는 S를 성공적으로 인증한다.

3.4 패스워드 변경 단계

이 단계는 사용자 U_i가 패스워드 P_i를 새로운 패스워드 P_{i_new}로 변경을 요청할 때 수행된다.

(1) U_i는 스마트카드를 카드 리더에 넣고 ID_i및 P_i를 입력하고 패스워드 변경을 요청한다.

(2) 스마트카드는 인증서버와의 상호작용에 의해 P_i의 유용성을 확인하고, 성공하면, $R(=X_s\oplus h(b\oplus P_i))$을 $R\oplus h(b\oplus P_{i_new})$으로 변경한다.

IV. 제안한 인증 스킴의 안전성 분석

본 장에서는 본 논문에서 제안한 인증 스킴에서 패스워드 추측 공격(password guessing attack), 위조 공격(forgery attack)/위장 공격(impersonation attack), 그리고 재전송 공격(replay attack) 등에 대해 획득가능한 정보, 즉 합법적 사용자의 스마트카드 정보들과 인증 메시지들로부터 안전성을 분석하였다. 그리고 제안한 인증 스킴의 안전성과 계산복잡도를 Hu-Niu-Yang의 인증 스킴과 비교 분석하였다.

4.1 패스워드 추측 공격

본 논문에서 공격자가 패스워드를 획득할 수 있는 방법은 사용자의 스마트카드에 일시적으로 접근하여 스마트카드에 저장된 정보를 추출하고 합법적인 사용자의 메시지를 도청함으로써 오프라인 패스워드 추측 공격을 수행하는 것이다. 즉, 합법적인 사용자 메시지 $\{ID_i, M_i, C_2\}$와 인증서버 메시지 $\{M_s, C_3\}$, 그리고 스마트카드에서 불법 추출한 저장 정보 R, $h()$, b로부터 패스워드 P_i를 추측하는 것이다. 식(3.2)와 식(3.4)의 $M_i(=C_1\oplus N_i=(R\oplus h(b\oplus P_i))\oplus N_i)$에서 패스워드 P_i를 추측하는 것은 random nonce N_i값과 hash 함수 때문에 불가능하다.

4.2 위조 공격/위장 공격

공격자는 사용자 U_i의 로그인 메시지 $\{ID_i, M_i, C_2\}$를 $\{ID_i, M_i^*, C_2^*\}$로 위조하려고 시도할 수 있다. 그러나 이와 같은 위장 공격 시도는 인증단계 식(3.3)을 통과하지 못할 것이다. 왜냐하면, 공격자는 유용한 C_2를 계산하기 위하여 $h(ID_T\oplus x)$의 값을 얻을 수 있는 방법이 없기 때문이다.

4.3 재전송 공격

메시지 재전송 공격(replay attack)은 이전 세션의 메시지를 다음 세션에서 재전송하는 방법으로서 불법적인 사용자가 이전 세션의 메시지를 재사용하여 인증을 시도하는 공격이다.

즉, 본 논문에서 제안된 인증 스킴은 매 세션마다 새로운 random nonce Ni을 생성하기 때문에 공격자는 인증단계 식(3.3)과 식(3.5)을 통과하지 못할 것이다. 따라서 이전에 사용된 메시지 {IDi, Mi, C2}, {Ms, C3}을 이용한 재전송 공격은 불가능 하다.

4.4 비교 분석

본 장에서는 본 논문에서 제안한 인증 스킴의 안전성과 계산복잡도를 분석하기 위하여 Hu-Niu-Yang이 제안한 인증 스킴과 비교 분석하였다.

4.4.1 안전성 분석

본 논문에서 제안한 인증 스킴의 안전성을 분석하기 위하여 Hu-Niu-Yang의 인증 스킴과 비교분석하였다.

표 1. 안전성 분석
Table 1. Analysis of security

스킴	패스워드 추측 공격	위조/위장 공격	재전송 공격	상호 인증
Hu et al.'s 스킴	가능	가능	불가능	가능
제안한 스킴	불가능	불가능	불가능	가능

표 1에서 제시된 바와 같이, Hu-Niu-Yang의 인증 스킴은 일부 공격, 즉 패스워드 추측공격, 위장공격 등에 취약함을 알 수 있고, 본 논문에서 제안한 인증 스킴은 이와 같은 보안 취약점들을 해결한 개선된 인증 스킴임을 알 수 있다.

4.4.2 효율성 분석

본 논문에서 제안한 인증 스킴의 효율성을 분석하기 위하여 Hu-Niu-Yang이 제안한 인증 스킴과 비교 분석하였다. 모든 인증 스킴은 hash와 exclusive-OR 연산을 기반으로 구성되어 있다. exclusive-OR 연산은 매우 작은 계산을 요구되기 때문에 일반적으로 그 계산은 무시된다.

표 2. 계산복잡도 분석
Table 2. Analysis of computational complexity

스킴	등록과정	로그인과정	인증과정
Hu et al.'s 스킴	2T(h)+2T(⊕)	3T(h)+4T(⊕)	4T(h)+4T(⊕)
제안한 스킴	1T(h)+2T(⊕)	3T(h)+5T(⊕)	6T(h)+11T(⊕)

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

표 2에서 제시된 바와 같이, 본 논문에서 제안한 인증 스킴이 인증 스킴의 전과정, 즉 등록과정, 로그인과정, 그리고 인증과정에 대한 계산량이 Hu-Niu-Yang의 인증 스킴보다 많은 것을 알 수 있다. 이것은 본 논문에서 제안된 스킴이 패스워드 추측 공격, 위조 공격/위장 공격, 상호인증 등을 방지하기 위한 hash 및 exclusive-OR 연산이 제공되었기 때문이다. 이것은 단지 추가된 연산들만으로 높은 보안성을 제공하는 것은 상대적으로 가치가 있다고 생각할 수 있다.

V. 결 론

본 논문에서는 Hu-Niu-Yang에 의해 제안된 스마트카드를 이용한 사용자 인증 스킴은 공격자가 사용자의 스마트카드에 일시적으로 접근하여 저장된 정보를 추출할 수 있다는 가정하에 off-line 패스워드 추측공격이 가능함을 증명하였다. 또한 본 논문에서는 이와 같은 안전성 취약점들을 해결한 Hu-Niu-Yang의 스킴을 개선한 사용자 인증 스킴을 새로이 제안하였다. 제안한 사용자 인증 스킴은 패스워드 추측공격, 위조 및 위장공격, 그리고 재생공격 등이 불가능한 안전한 인증 스킴임을 알 수 있었고, 이와 같은 다양한 공격들을 방지하기 위하여 상대적으로 hash 및 exclusive-OR 연산이 더 필요함을 알 수 있었다.

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

참고문헌

[1] 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.

[2] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," Proceedings of Advances in Cryptology (CRYPTO 99), pp. 388 - 397, 1999.

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

[4] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, 24(11), pp. 770-772, 1981.
[5] C.C. Chang, T.C. Wu, "Remote password authentication with smart card," IEEE Proceedings-E, 138(3), pp. 165-168, 1991.
[6] 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.
[7] C.L. Hsu, "Security of two remote user authentication schemes using smart card," IEEE Transactions on Consumer Electronics, 49(4), pp. 1196-1198, 2003.
[8] J.Q. Liu, J. Sun, T.H. Li, "An enhanced remote login authentication with smart card," Proceedings of IEEE Workshop on Signal Processing Systems Design and Implementation, pp. 229-232, (11) 2005.
[9] 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, (9) 2007.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 신광철, "서비스거부공격에 안전한 OTP 스마트카드 인증 프로토콜," 한국컴퓨터정보학회 논문지, 제 12권, 제 6호, 201-206쪽, 2007년 12월.
[15] 안영화, 이강호, "스마트카드를 이용한 사용자 인증 스킴의 안전성 분석," 한국컴퓨터정보학회 논문지, 제 14권, 제 3호, 133-138쪽, 2009년 3월.
[16] 이영숙, 원동호, "스마트카드를 이용한 사용자 인증 스킴의 안전성 분석 및 개선," 한국컴퓨터정보학회 논문지, 제 15권, 제 1호, 139-147쪽, 2010년 1월.
[17] 최병훈, 김상근, 배제민, "다중체계_인증을 이용한 중요 시스템 보완 접근에 관한 연구," 한국컴퓨터정보학회 논문지, 제 14권, 제 7호, 73-80쪽, 2009년 7월.

저 자 소 개

서 정 만

1988년 8월~1993년 10월 :
엘지전자(주)연구소 주임연구원
1993년 11월~1999년 2월 :
삼성중공업 중앙연구소 선임연구원
2000년 3월~2002년 2월 :
극동정보대학 컴퓨터게임개발과 교수
2003년 : 충북대학교 컴퓨터공학과 박사
2002년~현재 :
한국재활복지 대학 컴퓨터 게임개발과 교수
관심분야 : 실시간처리, 게임프로그래밍, 가상현실, 데이터베이스

안 영 화

1990년 2월 :
성균관대학교 전자공학과 공학박사
1983년 3월~1990년 2월 :
해군사관학교 전자공학과 교수
2002년3월~2003년 2월 : FSU방문교수
1990년 ~ 현재 :
강남대학교 컴퓨터 미디어 정보공학부 교수
관심분야 : 정보보호, 네트워크 보안