韓國컴퓨터情報學會 論文誌
第16卷 第2號, 2011. 2.

2011-16-2-3-10

순방향 비밀성을 제공하는 사용자 인증 스킴에 관한 연구

안 영 화*

A Study on the User Authentication Scheme with Forward Secrecy

Young-Hwa An*

요 약

최근 Wang-Li 등[6]은 자신이 선택한 패스워드와 스마트카드를 이용하여 원격지에 있는 사용자를 인증할 수 있는 스킴을 제안하였다. 그러나 Wang-Li 등에 의해 제안된 스킴은 패스워드 기반 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 만족하지 못하고 있다. 본 논문에서는, Wang-Li 및 Yoon 등[7]의 인증 스킴에 대해 기술하였고, 공격자가 사용자의 스마트카드를 훔치거나 일시적으로 접근할 수 있는 경우에 Wang-Li 등의 인증 스킴은 off-line 패스워드 추측공격 및 위장공격에 취약하다는 것을 증명하였다. 그리고 이와 같은 보안 취약점을 해결하기 위하여 hash 함수와 ElGamal 서명기반의 개선된 사용자 인증 스킴을 제안한다. 비교분석 결과, 제안한 사용자 인증 스킴은 패스워드 추측공격, 위장 공격, 재전송 공격 등 다양한 공격에 대응할 수 있고, 순방향 비밀성을 제공하는 스킴임을 알 수 있다. 또한 계산량은 비교 인증 스킴들과 유사하나 보안 취약점을 개선한 스킴으로서 비교할 때 상대적으로 효율적이라 할 수 있다. 따라서 제안한 인증 스킴은 Wang-Li 및 Yoon 등의 인증 스킴보다 상대적으로 안전하고 효율적인 스킴임을 알 수 있다.

▸ Keyword : 사용자 인증, 스마트카드, 패스워드 추측공격, 순방향 비밀성

Abstract

Recently Wang-Li proposed the remote user authentication scheme using smart cards. But the proposed scheme has not been satisfied security requirements considering in the user authentication scheme using the password based smart card. In this paper, we described the Wang-Li and Yoon et al.'s authentication scheme simply, and we prove that the Wang-Li's scheme is vulnerable to a password guessing attack and impersonation attack in case that the attacker steals the user's smart card and extracts the information in the smart card. Accordingly, we propose the improved user authentication scheme based on the hash function and generalized ElGamal signature scheme that can withstand many possible attacks including a password guessing attack, impersonation attack and replay attack, and that can offer the function of forward

• 제1저자 : 안영화
• 투고일 : 2010. 11. 05, 심사일 : 2010. 12. 07, 게재확정일 : 2011. 01. 09.
* 강남대학교 컴퓨터미디어정보공학부(Div. of Computer and Media Engineering, Kangnam University)
※ 본 연구는 2009학년도 강남대학교 교내연구비 지원에 의해 이루어짐.

secrecy. The result of comparative analysis, the our proposed scheme is much more secure and efficient than the Wang-Li and Yoon et al.'s scheme.

▸ Keyword : User authentication, Smart card, Password guessing attack, Forward secrecy

Ⅰ. 서 론

최근 컴퓨터 네트워크의 급속한 발달과 함께 인증 기술은 인터넷과 같은 신뢰할 수 없는 네트워크상에서 원격 접근을 위한 보안의 중요한 분야이다. 사용자 인증 프로토콜은 서비스를 제공하는 서버와 이를 이용하려는 사용자 간에 서로 상대방의 신원을 확인하고 정당한 시스템과 사용자의 검증을 수행하는 프로토콜이다. 이와 같은 인증 프로토콜에 의하여 사용자는 사전에 서비스를 제공하는 시스템에 미리 자신의 신원을 확인받을 수 있는 정보를 등록하고, 언제든지 정당한 사용자로서 검증받고 시스템이 제공하는 서비스를 제공받을 수 있다.

1981년에 Lamport[1]는 검증을 위해 패스워드 테이블이 요구되는 패스워드 인증 스킴을 처음으로 제안하였다. 그러나 이와 같은 인증 스킴은 사용자의 합법성을 확인하기 위하여 인증 시스템에 검증 테이블이 유지되어야 하는 취약점을 갖고 있다. 만일 침입자가 서버에 불법적으로 접근할 수 있다면, 검증 테이블의 내용은 쉽게 수정될 수 있을 것이다. 그리고 2000년에 Hwang과 Li[2] 등은 검증 테이블이 필요 없는 스마트카드기반 새로운 인증 스킴을 제안하였다. 그 후 Hwang-Li의 인증 스킴을 개선한 효율적인 스마트카드 기반 인증스킴들이 제안되었다[3-5]. 최근에 Wang-Li 등[6]은 Yoon 등[7]의 인증 스킴, 즉 Hwang-Li 등의 인증 스킴을 개선한 일반화된 ElGamal 서명 스킴에 기반한 상호 인증 스킴의 취약점을 제시하고 새로운 인증 스킴을 제안하였다.

일반적으로 스마트카드 기반 패스워드 인증 스킴은 인증서버의 오버헤드는 줄이고 사용자는 오직 자신의 패스워드만을 기억할 필요가 있다. 로그인 메시지를 생성하고 전송하는 것 이외에도 스마트카드는 상호 인증을 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 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[9]과 Messerges 등[10]은 모든 스마트카드 안에 저장된 비밀정보는 전력소비를 모니터함으로서 추출될 수 있음을 지적하였다. 따라서 일단 카드를 분실하면 카드 안의 모든 정보는 노출된다.

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

본 논문에서는 Wang-Li 등이 제안한 개선된 스킴도 패스워드 추측 공격(password guessing attack) 및 위장 공격(impersonation attack)에 취약함을 보였다. 즉, 공격자가 사용자의 스마트카드에 불법적으로 접근할 수 있다면 스마트카드에 저장된 정보를 추출함으로서 패스워드 추측과 함께 합법적인 사용자 및 시스템으로 가장할 수 있음을 보였다. 또한 본 논문에서는 Wang-Li 등에 의해 제안된 인증 스킴의 특징들을 유지하면서 보안 취약점들을 개선한 스마트카드 기반 인증 스킴을 제안하였다.

본 논문의 구성은 다음과 같다. 제Ⅱ장에서는 Wang-Li 및 Yoon 등의 인증 스킴을 기술하고, 안전성을 분석하였다. 제Ⅲ장과 제Ⅳ장에서는 개선된 인증 스킴을 제안하고, 안전성을 분석하였다. 그리고 Ⅴ장에서 결론을 맺는다.

Ⅱ. Wang-Li 및 Yoon 등의 인증 스킴 및 안전성 분석

본 장에서는 Wang-Li 등[6]이 제안한 사용자 인증 스킴을 간단히 기술하고 안전성을 분석한다. 또한 비교 분석을 위해 Yoon 등[7]의 인증 스킴도 간단히 기술한다. 이 인증 스킴들은 세 개의 단계, 즉 등록 단계, 로그인 단계, 그리고 인증 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_s : 인증 서버의 비밀키
h() : 안전한 일방향 해시 함수
‖ : 연접

2.1 Wang-Li 등의 사용자 인증 스킴

2.1.1 등록 단계

사용자 U_i는 아이디 ID_i와 패스워드 PW_i를 선택하고 안전한 채널을 이용하여 리모트 시스템에게 제출한다. 리모트 시스템은 다음 단계들을 수행한다.

(1) 리모트 시스템은 h(), p, q, g 등을 선택한다. 여기서 p는 1024 비트 크기를 갖는 큰 소수이고, q는 160 비트 크기를 갖는 p-1의 소수 약수이다. 그리고 g는 유한체 GF(p) 상에서 위수 q의 원소이다. 또한 h()의 출력 비트 크기는 |q|이다.
(2) 리모트 시스템은 다음 수식(2.1)을 계산한다.

$$R_i=h(ID_i \| x_s)$$
$$X_i=R_i \oplus h(ID_i \| PW_i) \quad \cdots\cdots (2.1)$$

(3) 리모트 시스템은 스마트카드에 개별 정보 {ID_i, R_i, X_i, h(), p, q, g}를 저장하고 사용자 U_i에게 발급한다.

2.1.2 로그인 단계

사용자 U_i는 리모트 시스템으로부터 발급받은 스마트카드를 카드 리더기에 넣고 아이디 ID_i와 패스워드 PW_i를 입력한다. 그리고 스마트카드는 다음 단계들을 수행한다.

(1) 스마트카드는 랜덤 수 $r \in Z_q^*$를 생성하고 $t=g^r \bmod p$를 계산한다.
(2) 스마트카드는 다음 식(2.2)를 계산한다.

$$V_i=X_i \oplus h(ID_i \| PW_i)$$
$$W_i=h(V_i \oplus T) \quad \cdots\cdots (2.2)$$

여기서 T는 현재 time-stamp이다.

(3) 스마트카드는 $s=h(t \| W_i)$를 계산하고 메시지 $C_1=\{ID_i, t, s, T\}$를 리모트 시스템에게 전송한다.

2.1.3 인증 단계

인증 요청 메시지 C_1를 수신한 리모트 시스템과 스마트카드는 사용자와 리모트 시스템 간의 상호인증을 위해 다음 과정을 수행한다.

(1) 리모트 시스템은 ID_i 를 검증한다. 만약 형식이 유효하지 않으면 리모트 시스템은 사용자의 로그인 요청을 거절한다.
(2) 리모트 시스템은 T와 T′(시스템이 C_1을 수신한 시간) 사이에 시간 간격의 유효성을 검증한다. 만약 $(T'-T) \geq \Delta T$라면 리모트 시스템은 로그인 요청을 거절한다. 여기서 ΔT는 유용한 전송 시간이다.
(3) 리모트 시스템은 다음 식(2.3)을 계산하고 s′과 수신된 s를 비교한다. 만약 비교 값이 같으면 리모트 시스템은 로그인 요청을 받아들이고 다음 단계들을 수행한다.

$$V_i'=h(ID_i \| x_s)$$
$$W_i'=h(V_i' \oplus T)$$
$$s'=h(t \| W_i') \quad \cdots\cdots (2.3)$$

(4) 리모트 시스템은 랜덤 수 $r' \in Z_q^*$를 생성하고 세션키 $k=t^{r'} \bmod p$를 계산한다.
(5) 리모트 시스템은 다음 수식(2.4)를 계산하고 사용자 U_i에게 메시지 $C_2=\{u, v, T''\}$를 전송한다.

$$w=h(V_i' \oplus T'')$$
$$u=g^{r'} \bmod p$$
$$v=h(u \| w) \quad \cdots\cdots (2.4)$$

여기서 T″는 현재 time-stamp이다.

(6) 메시지 {u, v, T″}를 수신한 스마트카드는 T″와 현재 time-stamp T‴간 시간 간격의 유용성을 검증한 후, 다음 수식(2.5)를 계산한다.

$$w'=h(V_i' \oplus T'')$$
$$v'=h(u \| w') \quad \cdots\cdots (2.5)$$

만약 v=v′이면 상호인증을 성공적으로 완성한다. 그리고 사용자 U_i와 리모트 시스템 사이의 세션키 $k=g^{rr'} \bmod p$를

계산한다.

2.1.4 패스워드 변경 단계

사용자 U_i가 패스워드 PW_i를 새로운 패스워드 PW_i'로 변경을 요청할 경우, 사용자 U_i는 스마트카드를 카드 리더기에 넣고 아이디 ID_i와 패스워드 PW_i를 입력한다. 그리고 스마트카드는 다음 단계들을 수행한다.

(1) 스마트카드는 $V_i=X_i \oplus h(ID_i \| PW_i)$를 계산하고 스마트카드에 저장된 R_i와 비교한다.
(2) 만약 같으면, 사용자 U_i는 새로운 패스워드 PW_i'를 입력한다. 그렇지 않으면 패스워드 변경 요청을 거절한다.
(3) 스마트카드는 $X_i'=V_i \oplus h(ID_i \| PW_i')$를 계산하고, 스마트카드에 저장된 X_i 대신에 X_i'를 저장한다.

2.2 Yoon 등의 인증 스킴

2.2.1 등록 단계

사용자 U_i는 아이디 ID_i와 패스워드 PW_i를 선택하고 리모트 시스템에게 제출한다. 그 다음에 리모트 시스템은 다음 단계들을 수행한다.

(1) $VPW_i=g^{xs} \bmod p$를 계산한다. 여기서 p는 q, 그리고 g는 2.1.1절에 기술한 파라메터와 동일하다.
(2) 리모트 시스템은 다음 수식(2.6)을 계산한다.

$$R_i=h(ID_i,x_s)$$
$$X_i=R_i \oplus h(ID_i,PW_i) \quad \cdots\cdots (2.6)$$

(3) 리모트 시스템은 생성된 개별정보 $\{ID_i, VPW_i, R_i, X_i, h(), p, q, g\}$를 스마트카드에 저장하고 사용자 U_i에게 스마트카드를 발급한다.

2.2.2 로그인 단계

사용자 U_i는 발급받은 스마트카드를 카드 리더기에 넣고 아이디 ID_i와 패스워드 PW_i를 입력하고, 다음 단계들을 수행한다.

(1) 스마트카드는 랜덤 수 $r \in Z_q^*$를 생성하고, 다음 식(2.7)을 계산한다.

$$k=(VPW_i)^r \bmod p$$
$$t=h(k, T) \quad \cdots\cdots (2.7)$$

(2) 그 다음에 스마트카드는 다음 식(2.8)를 계산하고, 생성된 메시지 $C_1=\{ID_i, t, s, T\}$를 리모트 시스템에게 전송한다.

$$V_i=X_i \oplus h(ID_i,PW_i)$$
$$s=r-V_i^t \bmod q \quad \cdots\cdots (2.8)$$

2.2.3 인증 단계

인증 요청 메시지 C_1를 수신한 리모트 시스템과 스마트카드는 다음 단계들과 같이 상호인증을 수행한다.

(1) 리모트 시스템은 ID_i 형식 및 T와 T′ 사이에 시간 간격의 유효성을 검증한다.
(2) 리모트 시스템은 다음 식(2.9)을 계산하고 t와 $h(k', T)$를 비교한다. 만약 비교 값이 같으면 리모트 시스템은 로그인 요청을 받아들이고 다음 단계를 수행한다.

$$V_i'=h(ID_i,x_s)$$
$$k'=(g^s g^{vi't})^{xs} \bmod p \quad \cdots\cdots (2.9)$$

(3) 리모트 시스템은 식 $C_2=h(k', V_i', T'')$를 계산하고 생성된 메시지 $\{C_2, T''\}$를 사용자 U_i에게 전송한다.
(4) 메시지 $\{C_2, T''\}$를 수신한 스마트카드는 T″와 현재 time-stamp T‴간 시간 간격의 유용성을 검증한 후, $C_2'=h(k, V_i, T'')$과 C_2를 비교한다. 만약 그 값이 동일하면 상호인증을 성공적으로 완성한다.

2.3 안전성 분석

본 절에서는 Wang-Li의 인증 스킴에 대해서 패스워드 추측공격(password guessing attack) 및 위장 공격(impersonation attack) 등에 대하여 안전성을 분석한다.

2.3.1 패스워드 추측공격(password guessing attack)

이 공격을 수행하기 위해 공격자는 합법 사용자의 스마트카드를 훔치거나 일시적으로 접근하여 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정한다. 따라서 공격자 U_a는 합법 사용자 U_i의 스마트카드로부터 ID_i, R_i, X_i, h()를 획득한 후, 다음 단계들과 같이 off-line 패스워드 추측공격으로 합법 사용자 U_i의 패스워드 PW_i를 추측할 수 있다.

(1) 공격자 U_a는 합법 사용자 U_i의 로그인 요청 메시지 C_1={ID_i, t, s, T}를 불법 획득한다.
(2) 그리고 합법 사용자 U_i의 패스워드를 PW_i'로 추측하고, $s'=h(t \| W_i')=h(t \| h(X_i \oplus h(ID_i \| PW_i')) \oplus T))$를 계산한다.
(3) 공격자 U_a는 계산된 s′와 불법 획득한 s가 동일한 값을 갖는 지 확인한다.
(4) 공격자 U_a는 추측한 s′가 (3)의 조건을 만족할 때까지 (2), (3) 과정을 반복 수행한다. 이때 (3)의 조건을 만족하면, 추측된 패스워드 PW_i'는 합법 사용자 U_i의 올바른 패스워드가 된다.

또한, 공격자 U_a는 스마트카드로부터 불법 획득한 D_i, R_i, X_i, h()와 합법 인증 서버 S의 인증 요청 메시지 C_2={u, v, T″}의 v(=h(u ‖ w))에서 상기와 같이 동일한 방법을 사용하여 합법 사용자 U_i의 패스워드 PW_i를 off-line 패스워드 추측 공격으로 찾아낼 수 있다.

이와 같이 Wang-Li 등의 인증 스킴은 합법 사용자 U_i의 스마트카드를 훔치거나 일시적으로 접근하여 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정할 경우, off-line 패스워드 추측 공격 방식을 이용하면 사용자의 패스워드를 용이하게 찾아 낼 수 있다. 따라서 Wang-Li의 인증 스킴은 사용자 인증 스킴에서 고려하는 보안 요구사항을 충족하지 못하고 있음을 알 수 있다.

2.3.2 위장 공격(impersonation attack)

2.3.1절에서 기술된 패스워드 추측공격 방법을 통하여 PW_i를 얻게 되면, 공격자 U_a는 사용자와 원격 인증서버 간의 비밀정보인 $h(ID_i \| x_s)$을 획득할 수 있다. 또한 공격자 U_a는 합법 사용자 U_i의 스마트카드로부터 R_i(=V_i)를 획득할 수 있다. 이와 같이 불법적인 방법으로 $h(ID_i \| x_s)$를 획득한 공격자 U_a는 새로운 로그인 메시지 C_{1a}={ID_i, t_a, s_a, T_a}를 생성하여 원격 인증 서버 S에게 보냄으로서 합법적인 사용자 U_i로 위장할 수 있다. 또한 $h(ID_i \| x_s)$를 불법적으로 획득한 공격자 U_a는 새로운 서버 인증 메시지 C_{2a}={u_a, v_a, T_a''}를 생성하여 원격 사용자 U_i에게 보냄으로서 합법적인 원격 인증서버 S로 위장할 수 있다. 따라서 Wang-Li의 스킴은 위장 공격에 취약함으로서 사용자 인증 스킴에서 고려하는 보안 요구사항을 충족하지 못하고 있음을 알 수 있다.

III. 제안한 인증 스킴

본 장에서는 2.3절에서 기술된 Wang-Li 스킴의 보안 취약점들을 개선한 사용자 인증 스킴을 새로이 제안하였다. 제안된 인증 스킴의 안전성은 hash 함수와 ElGamal 서명 기반이며, 그림 1과 같이 등록 단계, 로그인 단계, 인증 단계, 그리고 패스워드 변경 단계로 구성된다.

3.1 등록 단계

이 단계는 사용자 U_i가 인증 서버 S에 등록하고자 할 때 수행되며, 사용자 U_i는 자신의 아이디 ID_i와 패스워드 PW_i를 선택하고 안전한 채널을 이용하여 인증 서버에 제출하고, 다음 단계들을 수행한다.

(1) 리모트 시스템은 h(), p, q, g 등을 선택한다. 여기서 p는 1024 비트 크기를 갖는 큰 소수이고, q는 160 비트 크기를 갖는 p-1의 소수 약수이다. 그리고 g는 유한체 GF(p) 상에서 위수 q의 원소이다. 또한 h()의 출력 비트 크기는 | q | 이다.

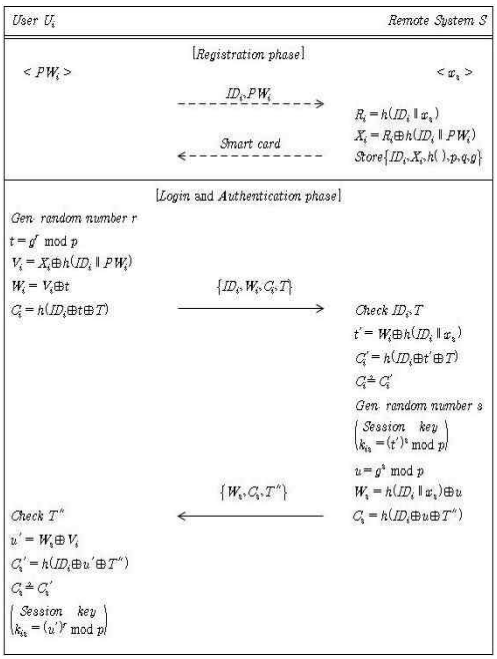

그림 1. 제안한 인증 스킴
Fig 1. The our proposed scheme

(2) 사용자의 등록 요청 정보를 수신한 인증 서버 S는 다음과 같이 수식(3.1)을 계산한다.

$R_i=h(ID_i \| x_s)$

$$X_i=R_i \oplus h(ID_i \| PW_i) \quad \cdots\cdots (3.1)$$

여기서 x_s는 시스템의 비밀 키이다.

(3) 인증 서버 S는 개별 정보 {ID_i, X_i, h(), p, g}를 저장한 스마트카드를 사용자 U_i에게 발급한다.

3.2 로그인 단계

이 단계는 사용자 U_i가 로그인하여 인증 서버에게 인증 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) 랜덤 수 $r \in Z_q^*$를 생성하고, 식(3.2)를 계산한다.

$$t=g^r \bmod p \quad \cdots\cdots (3.2)$$

(2) 스마트카드는 다음 식(3.3)을 계산한다.

$$V_i=X_i \oplus h(ID_i \| PW_i)$$
$$W_i=V_i \oplus t$$
$$C_i=h(ID_i \oplus t \oplus T) \quad \cdots\cdots (3.3)$$

여기서 T는 현재 time-stamp이다.

(3) 스마트카드는 사용자 U_i의 로그인 요청 메시지 {ID_i, W_i, C_i, T}를 인증 서버 S에게 전송한다.

3.3 인증 단계

인증 요청 메시지{ID_i, W_i, C_i, T}를 수신한 인증 서버 S와 스마트카드는 사용자와 인증 서버 사이의 상호인증을 위해 다음 과정을 수행한다.

(1) 리모트 시스템은 ID_i 를 검증한다. 만약 유효하지 않으면 리모트 시스템은 사용자의 로그인 요청을 거절한다.

(2) 또한 리모트 시스템은 T와 T′(시스템이 C_i을 수신한 시간) 사이에 시간 간격의 유효성을 검증한다. 만약 $(T'-T) \leqq \Delta T$라면 리모트 시스템은 로그인 요청을 승인한다. 여기서 ΔT는 유용한 전송 시간이다.

(3) 리모트 시스템은 다음 식(3.4)를 계산하고 C_i'과 수신된 C_i를 비교한다. 만약 비교 값이 같으면 리모트 시스템은 사용자 U_i를 인증하고 다음 단계를 수행한다.

$$t'=W_i \oplus h(ID_i \| x_s)$$
$$C_i'=h(ID_i \oplus t' \oplus T) \quad \cdots\cdots (3.4)$$

(4) 리모트 시스템은 랜덤 수 $s \in Z_q^*$를 생성하고 세션키 $k_{is}=t^s \bmod p$를 계산한다.

(5) 리모트 시스템은 다음 수식(3.5)를 계산하고 사용자 U_i에게 메시지 {W_s, C_s, T″}를 전송한다.

$$u=g^s \bmod p$$
$$W_s=h(ID_i \| x_s) \oplus u$$
$$C_s=h(ID_i \oplus u \oplus T'') \quad \cdots\cdots (3.5)$$

여기서 T″는 현재 time-stamp이다.

(5) 메시지 {W_s, C_s, T″}를 수신한 스마트카드는 T″와 현재 time-stamp T‴간 시간 간격의 유용성을 검증한 후, 다음 수식(3.6)을 계산한다.

$$u'=W_s \oplus V_i$$
$$C_s'=h(ID_i \oplus u' \oplus T'') \quad \cdots\cdots (3.6)$$

만약 $C_s'=C_s$이면 상호인증을 성공적으로 완성한다. 그리고 사용자 U_i와 리모트 시스템 사이의 세션키 $k_{is}=g^{rs} \bmod p$를 계산한다.

3.4 패스워드 변경 단계

사용자 U_i가 패스워드 PW_i를 새로운 패스워드 PW_{i_new}로 변경을 요청할 경우, 다음과 같이 수행된다.

(1) 사용자 U_i는 스마트카드를 카드 리더에 넣고 ID_i 및 PW_i를 입력하고, $R_i(=X_i \oplus h(ID_i \| PW_i))$를 계산한다.

(2) 스마트카드는 인증 서버와의 상호작용에 의해 PW_i의 유용성을 확인하고, 성공하면 사용자 U_i는 새로운 패스워드 PW_{i_new}를 선택한다.

(3) 스마트카드는 $X_{i_new}(=R_i \oplus h(ID_i \| PW_{i_new}))$를 계산하고, 스마트카드에 저장된 X_i 대신에 X_{i_new}를 저장한다.

IV. 제안한 인증 스킴의 안전성 분석

본 장에서는 제안한 사용자 인증 스킴에서 패스워드 추측 공격(password guessing), 위장 공격(impersonation attack), 재전송 공격(replay attack), 그리고 순방향 비밀성(foreard secrecy) 등에 대해 안전성을 분석하였다. 그리고 제안한 인증 스킴의 안전성을 Wang-Li[6] 및 Yoon 등[7]의 인증 스킴과 비교 분석하였다.

4.1 패스워드 추측공격

본 논문에서 공격자가 패스워드를 획득할 수 있는 방법은 사용자의 스마트카드에 일시적으로 접근하여 스마트카드에 저장된 정보를 추출하고 합법적인 사용자의 메시지를 도청함으로써 오프라인 패스워드 추측공격을 수행하는 것이다. 즉, 합법적인 사용자의 메시지 {ID_i, W_i, C_i, T}와 {W_s, C_s, T″}, 그리고 스마트카드 저장 정보 {IDi, X_i, h(), p, g}로부터 패스워드를 추측하는 것이다. 식(3.3)의 $W_i(=V_i \oplus t=X_i \oplus h(ID_i \| PW_i) \oplus t)$에서 패스워드 PW_i'를 추측하는 것은 랜덤 값 t와 hash 함수 때문에 불가능하다.

4.2 위장 공격

공격자 U_a는 합법적인 사용자 U_i로 위장하기 위하여 위조된 메시지 {ID_i, W_{ia}, C_{ia}, T_a}를 원격 인증 서버 S에게 보냄으로서 합법적인 사용자 U_i로 위장할 수 있다. 그러나 사용자 인증단계 식(3.4)에서 C_i'를 계산하기 위하여 시스템 비밀 값 x_s를 얻을 수 있는 방법이 없기 때문에 사용자 인증에 실패할 것이다. 또한 공격자 U_a는 합법적인 원격 인증 서버 S로 위장하기 위하여 위조된 메시지 {W_{sa}, C_{sa}, T_a''}를 원격 사용자 U_i에게 보냄으로서 합법적인 원격 인증 서버 S로 위장할 수 있다. 그러나 서버 인증단계 식(3.6)에서 C_s'를 계산하기 위하여 시스템 비밀 값 x_s 또는 PW_i를 얻을 수 있는 방법이 없기 때문에 서버 인증에 실패할 것이다.

4.3 재전송 공격

메시지 재전송 공격은 이전 세션의 메시지를 다음 세션에서 재전송하는 방법으로서 불법적인 사용자가 인증을 시도하는 공격이다. 본 논문에서 제안된 인증 스킴은 매 세션마다 새로운 랜덤 값 t, u 및 time stamp T, T″를 생성하기 때문에 공격자의 재전송 공격은 인증 단계 식(3.4)과 식(3.6)를 통과하지 못할 것이다. 따라서 이전 세션의 메시지 정보 {ID_i, W_i, C_i, T}와 {W_s, C_s, T″}를 이용한 재전송 공격은 불가능하다.

4.4 순방향 비밀성

시스템의 비밀키 x_s가 몇가지 이유로 인하여 공격자에게 노출되었다고 가정한다. DH 문제[11]의 어려움에 기반하여, 침입자가 주어진 정보, (g, g^r, g^s)로부터 인증단계에서 상호 교환된 세션키 $k_{is}=g^{rs} \bmod p$를 유추한다는 것은 계산적으로 불가능하다. 따라서 제안된 인증 스킴은 순방향 비밀성을 갖는다.

4.5 비교 분석

본 장에서는 본 논문에서 제안한 인증 스킴의 안전성과 계산복잡도를 분석하기 위하여 Wang-Li 및 Yoon 등의 인증 스킴과 비교 분석하였다.

4.5.1 안전성 분석

본 논문에서 제안한 인증 스킴의 안전성을 분석하기 위하여 안전성 위협요소 및 안전성 향상요소들을 비교 분석하였다.

표 1. 안전성 분석
Table 1. Analysis of security

스킴	패스워드 추측 공격	위장공격	재전송 공격	순방향 비밀성
Yoon 등의 스킴	가능	가능	불가능	불가능
Wing-Li의 스킴	가능	가능	불가능	가능
제안한 스킴	불가능	불가능	불가능	가능

표 1에서 비교된 바와 같이, Wang-Li 및 Yoon 등의 인증 스킴은 일부 공격, 즉 패스워드 추측공격, 위장공격 등에 취약함을 알 수 있고, 본 논문에서 제안한 인증 스킴은 이와 같은 보안 취약점들을 해결하고 순방향 비밀성이 가능한 개선된 인증 스킴임을 알 수 있다.

4.5.2 계산복잡도 분석

본 논문에서 제안한 인증 스킴의 효율성을 분석하기 위하여 인증 스킴의 전 과정에 대해 계산량을 비교 분석하였다. 제시된 인증 스킴들은 hash와 exclusive-OR, 그리고 지수연산을 기반으로 구성되어 있다.

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

스킴	등록단계	로그인단계	인증단계	패스워드변경 단계
Yoon 등의 스킴	2T(h)+1T (⊕)+1T(E)	2T(h)+1T (⊕)+1T(E)	4T(h)+2T(E)	2T(h)+2T (⊕)

Wing-Li의 스킴	2T(h)+1T (⊕)	3T(h)+2T (⊕)+1T(E)	7T(h)+3T (⊕)+3T(E)	2T(h)+2T (⊕)
제안한 스킴	2T(h)+1T (⊕)	2T(h)+4T (⊕)+1T(E)	5T(h)+9T (⊕)+3T(E)	2T(h)+2T (⊕)

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

표 2에서 제시된 바와 같이, 본 논문에서 제안한 인증 스킴은 인증 스킴의 모든 단계, 즉 등록단계, 로그인단계, 인증단계, 그리고 패스워드 변경단계에 대한 계산량 정도는 Wang-Li 및 Yoon 등의 인증 스킴과 비교할 때 유사하나, 안전성 분석에서 보여지듯이 보안 취약점들을 해결한 개선된 스킴으로서 비교할 때 상대적으로 효율적이라 할 수 있다. 일반적으로 인증 스킴에서 exclusive-OR 연산은 매우 작은 계산시간이 요구되기 때문에 그 계산은 무시할 수 있다.

V. 결 론

스마트카드를 이용한 사용자 인증 스킴은 공격자가 사용자의 스마트카드 내부에 저장된 정보를 추출하여도 그 정보를 이용하여 사용자의 패스워드를 알아내는데 이용하거나 사용자인척 하거나 또는 서버인척 할 수 없도록 설계되어야 한다.

본 논문에서는 Wang-Li 등에 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 ElGamal 서명 기반의 개선된 사용자 인증 스킴을 제안하였다. 제안한 사용자 인증 스킴은 패스워드 추측공격(password guessing attack), 위장 공격(impersonation attack), 그리고 재전송 공격(replay attack)등 다양한 공격을 방어할 수 있고, 또한 순방향 비밀성(forward secrecy) 기능을 제공한다. 비교분석 결과, 제안한 인증 스킴은 Wang-Li 및 Yoon 등의 인증 스킴보다 다수의 보안 취약점들을 해결하였고, 계산량에서 상대적으로 효율적인 스킴임을 알 수 있었다.

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

참고문헌

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

[2] M.S. Hwang, L.H. Li, "A New remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron, 46(1), Feb. 2000.

[3] C.K Chan, L.M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron, 46(4), pp. 992-993, Nov. 2000.

[4] J.J Shen, C.W.Lin, and M.S. Whang, "A modified remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron, 46(2), pp. 414-416, May. 2003.

[5] Zuhua Shao, "Efficient deniable authentication protocol based on generalized ElGamal signature scheme," Computer Standards & Interfaces, Article in press, Dec. 2003.

[6] B. Wang, ZQ. Li, "Forward-secure user authentication scheme with smart cards," International Journal of Network Security, Vol. 3, No. 2, pp. 116-119, Sept. 2006.

[7] E.J. Yoon, E.K. Ryu, K.Y. Yoo, "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," IEEE Trans. Consum. Electron, 50(2), pp. 568-570, 2004.

[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 - 397, 1999.

[10] 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.

[11] W. Diffie and M. Hellman, "New directions in

cryptography," IEEE Transactions on Information Theory, vol. IT-22, pp. 644 - 654, 1976.

[12] Y.S. Lee, D.H. Won, "Cryptanalysis and enhancement of a remote user authentication scheme using smart cards," Journal of The Korea Society of Computer and Information, Vol. 15, No. 1, pp. 139-147, Jan. 2010.

저 자 소 개

안 영 화

1975 : 성균관대학교
전자공학과 공학사

1977 : 성균관대학교
전자공학과 공학석사

1990 : 성균관대학교
전자공학과 공학박사

현 재 : 강남대학교
컴퓨터미디어정보공학부 교수

관심분야 : 정보보호, 네트워크 보안

Email : yhan@kangnam.ac.kr