Journal of the Korea Academia-Industrial Cooperation Society
Vol. 12, No. 12 pp. 5895-5901, 2011

http://dx.doi.org/10.5762/KAIS.2011.12.12.5895

패스워드 추측공격에 안전한 원격 사용자 인증 스킴

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

Secure Remote User Authentication Scheme for Password Guessing Attack

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 본 논문에서는 An[7]이 제안한 스킴이 패스워드 기반 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 만족하지 못함을 보였다. 이러한 보안 취약점을 해결하기 위하여 해시함수와 ElGamal 서명기반의 개선된 사용자 인증 스킴을 제안한다. 제안한 사용자 인증 스킴은 패스워드 추측공격, 위장공격, 재전송공격에 대응할 수 있고, 순방향 비밀성을 제공하는 스킴이다. 제안한 스킴은 An의 인증 스킴과 비교할 때,계산복잡도는 별 차이가 없이 유사하나, 안전성은 상대적으로 효율적임을 알 수 있다.

Abstract This paper shows that a scheme provided by An[7] is not enough to satisfy security requirements for a user certification using a password-based smart card. In order to compensate this weakness, this study provides an improved user scheme with a hash function and ElGamal signature. This new scheme has some advantages protecting password guessing attack, masquerade, and replay attack as well as providing forward secrecy. Compared to An's certification scheme, this scheme suggests that the effect of computational complexity is similar but the efficiency of safety is better.

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

1. 서론

사용자 인증 프로토콜은 서비스를 제공하는 서버와 서비스를 이용하려는 사용자간에 서로 상대방의 신원을 확인하고 정당한 사용자와 서버라는 검증을 수행하는 프로토콜이다. 인터넷과 같이 신뢰할 수 없는 네트워크상에서 원격 접근을 위해서는 사용자 인증 프로토콜이 보안에서 매우 중요한 역할을 한다. 사용자 인증 프로토콜에 의하여 정당한 사용자는 서비스를 제공하는 시스템에 미리 자신의 신원을 확인받을 수 있는 정보를 등록하고, 언제든지 정당한 사용자로서 검증 받고 시스템이 제공하는 서비스를 이용할 수 있다.

1981년에 Lamport[1]는 암호화 기법을 사용하지 않는 패스워드 기반의 원격 사용자 인증 스킴을 처음으로 제안하였고, 1993년에 Chang-Wu[2]등은 스마트카드를 갖는 원격 패스워드 인증 스킴을 소개했다. 그 이후 스마트카드 기반 원격 패스워드 인증 스킴은 안전성 또는 효율성을 개선하기 위해 다수 제안되었다.

Lamport가 제안한 인증 스킴은 사용자의 합법성을 확인하기 위하여 인증 시스템에 검증 테이블이 유지되어야 하는 취약점을 갖고 있다. 2002년에 Hwang-Li[3]은 검증 테이블이 필요 없는 스마트기반의 인증 스킴을 제안하였다. 그 후에 개선된 많은 스마트기반의 인증 스킴들이 제안되었다[4].[5]. Wang-Li[6]은 Hwang-Li의 인증 스킴을 개선한 일반화된 ElGamal 서명 스킴에 기반한 상호인증 스킴의 취약점을 제시하고 새로운 인증 스킴을 제안하였다.

An[7]은 Wang-Li등이 제안한 인증 스킴에서 패스워드

*교신저자 : 신승수(shinss@tu.ac.kr)
접수일 11년 09월 05일 수정일 (1차 11년 09월 26일, 2차 11년 10월 05일, 3차 11년 10월 07일) 게재확정일 11년 12월 13일

추측공격, 위장공격, 재전송공격, 순방향 비밀성에 대한 안전성을 분석하였고, 그 중에서 패스워드 추측공격과 위장공격이 가능하다는 것을 보였다. 패스워드 추측공격과 위장공격에 취약함을 보이고, 이를 개선한 인증 스킴을 제안 하였으나, An이 제안한 인증 스킴 역시 패스워드 추측공격과 위장공격에 취약하다. 본 논문에서는 An에 의해 제안된 인증 스킴의 특징을 유지하면서 보안 취약점들을 개선한 인증 스킴을 제안한다.

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

2. An의 인증 스킴 분석

An은 Wang-Li등의 인증 스킴이 패스워드 추측공격과 위장공격에 취약함을 다음과 같이 분석하였다. 먼저, 오프라인 패스워드 추측공격에 대하여 분석하였다. 오프라인 패스워드 추측공격을 수행하기 위해 공격자는 정당한 사용자의 스마트카드를 훔치거나 일시적으로 접근하여 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정한다[9][10]. 따라서 공격자는 정당한 사용자의 스마트카드에 저장된 정보를 획득한 후, 오프라인 패스워드 추측공격으로 정당한 사용자의 패스워드를 추출할 수 있음을 보였다. 그러나 An의 인증 스킴 역시 오프라인 패스워드 추측공격과 위장공격에 취약함을 보이기 위해서 An의 인증 스킴에 대하여 알아보고, 취약성을 분석하였다.

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. 스마트카드 기반 사용자 인증 스킴의 안전성을 평가하기 위해 공격자는 다음과 같은 능력을 갖고 있다고 가정한다[8].

공격자는 로그인단계 및 인증단계에서 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) 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 스마트카드가 일시적으로 도난당했으나 패스워드는 공격자에게 노출되지 않은 경우에 스마트카드 기반 패스워드 인증 스킴에 대해 논의한다.

An은 Wang-Li의 인증 스킴이 패스워드 추측공격과 위장공격에 취약함을 보이고 이를 개선한 새로운 스킴을 제안하였다. An에 의해 제안된 스킴의 안전성은 해시함수와 ElGamal 서명기반이며, 다음과 같이 등록단계, 로그인단계, 인증단계, 그리고 패스워드 변경단계로 구성된다.

2.1 An의 인증 스킴

<등록단계>

이 단계는 사용자 U_i가 인증서버 S에 등록을 할 때 수행되며, 사용자 U_i는 자신의 아이디 ID_i와 패스워드 PW_i를 선택하고 안전한 채널을 이용하여 인증서버에 제출하고, 다음 단계들을 수행한다.

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

2) 사용자 U_i의 등록 요청을 수신한 인증서버 S는 다음을 계산한다.

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

여기서, x_s는 서버의 비밀키이다.

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

<로그인단계>

이 단계는 사용자 U_i가 로그인하여 인증서버에게 인증받으려고 할 때마다 수행된다. 사용자 U_i는 스마트카드를 카드리더기에 넣고 아이디 ID_i와 패스워드 PW_i를 입력한다. 그리고 스마트카드는 다음 단계들을 수행한다.

1) 랜덤 수 $r \in Z_q^*$를 생성하고 다음을 계산한다.

$$t \equiv g^r \bmod p$$

2) 스마트카드는 다음을 계산한다.

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

여기서, T는 스마트카드의 현재 타임스탬프이다.

3) 스마트카드는 사용자 U_i의 로그인 요청 메시지 {ID_i, W_i, C_i, T}를 인증서버에 전송한다.

<인증단계>

인증요청 메시지 {ID_i, W_i, C_i, T}를 수신한 인증 서버와 스마트카드는 사용자와 인증서버 사이의 상호인증을 위해 다음 과정을 수행한다.

1) 원격시스템은 아이디 ID_i를 검증한다. 만약 형식이 유효하지 않으면 원격시스템은 사용자의 로그인 요청을 거절한다,
2) 원격시스템은 T와 T'(시스템이 C_i을 수신한 시간)사이에 시간 간격의 유효성을 검증한다. 만약 (T'-T)≤ △T라면 원격시스템은 로그인 요청을 승인한다. 여기서, △T는 유효한 전송 시간이다.
3) 원격시스템은 C_i'를 계산하고 C_i'과 수신한 C_i를 비교한다. 만약 비교 값이 같으면 원격시스템은 사용자 U_i를 인증하고 다음 단계를 수행한다.
$$t'=W_i\oplus h(ID_i \| x_s),\ C_i'=h(ID_i\oplus t'\oplus T)$$
4) 원격 시스템은 랜덤 수 $s\in Z_q^*$를 생성하고 세션키 $k\equiv t^s \bmod p$를 계산한다.
5) 원격시스템은 다음 수식을 계산하고 사용자 U_i에게 메시지 {W_s, C_s, T"}를 전송한다.
$$u\equiv g^s \bmod p,\quad W_s=h(ID_i \| x_s)\oplus u,$$
$$C_s=h(ID_i\oplus u\oplus T")$$
여기서, T"는 현재 원격시스템의 타임스탬프이다.
6) 메시지 {W_s, C_s, T"}를 수신한 스마트카드는 T"와 현재 타임스탬프 T'"간 시간 간격의 유효성을 검증한 후, 다음 수식을 계산한다.
$$u'=W_s\oplus V_i,\quad C_s'=h(ID_i\oplus u'\oplus T'")$$

만약, C_s=C_s'이면 상호인증을 성공적으로 완성한다. 그리고 사용자 U_i와 원격시스템 사이의 세션키 $k\equiv g^{rs} \bmod p$를 계산한다.

<패스워드 변경단계>

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

1) 사용자 U_i는 스마트카드를 카드리더에 넣고 아이디 ID_i와 패스워드 PW_i를 입력하고, $R_i(=X_i\oplus h(ID_i \| PW_i)$를 계산한다.
2) 스마트카드는 인증서버와 상호작용에 의해 PW_i의 유효성을 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.

2.2 An의 안전성 분석

이 절에서는 An이 제안한 스킴에 대해 패스워드 추측공격과 위장공격에 대해 분석한다.

2.2.1 패스워드 추측공격 분석

An은 Wang-Li에 의해 제안된 스마트카드를 이용한 사용자 인증 스킴이 패스워드 추측공격에 취약함을 지적하였다. 그러나 An의 인증 스킴 역시 패스워드 추측공격에 취약함에 대해 분석한다. 패스워드 추측공격은 온라인과 오프라인 패스워드 추측공격으로 나눌 수 있다. 온라인 패스워드 추측공격은 인증 실패 횟수를 계산함으로써 쉽게 탐지되고 조치될 수 있다.

본 논문에서는 오프라인 패스워드 추측공격에 대해서만 고려하여 분석한다. 오프라인 패스워드 추측공격을 수행하기 위해 공격자 U_a는 정당한 사용자 U_i의 스마트카드를 훔치거나 일시적으로 접근하여 카드 안에 저장되어 있는 정보를 추출할 수 있다고 가정한다. 따라서 정당한 사용자 U_i의 스마트카드로부터 추출한 정보를 이용하여 공격자 U_a는 다음과 같은 과정으로 사용자 U_i의 패스워드 PW_i를 알아낼 수 있다.

1 : 공격자 U_a는 정당한 사용자 U_i의 로그인 요청 메시지 {ID_i, W_i, C_i, T}를 불법 획득한다.
2 : 이때 공격자 U_a는 정당한 사용자 U_i의 로그인 요청 메시지를 가로채서 W_i과 C_i를 획득한다.
3 : 공격자 U_a는 획득한 정보를 이용하여 오프라인 패스워드추측 공격을 수행한다.
   (1) 공격자 U_a는 정당한 사용자 U_i의 패스워드 PW_i'로 추측한다.
   (2) 스마트카드로부터 추출한 정보 X_i과 PW_i'로부터 $X_i\oplus h(ID_i \| PW_i')=V_i'$를 계산한다.
   (3) 그리고 $t'=W_i\oplus V_i'$를 계산한다.
   (4) 공격자 U_a는 V_i'과 t'를 이용하여 $C_i'=h(ID_i\oplus t'\oplus T)$를 계산한다.
   (5) 계산한 C_i'와 불법 획득한 C_i가 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.

2.2.2 위장공격 분석

다음은 위장공격에 대하여 취약함을 분석한다. 오프라인 패스워드 추측공격 방법을 통하여 패스워드 PW_i를 얻게 되면 공격자 U_a는 정당한 사용자 U_i와 원격 시스템 S 간의 비밀정보인 $h(ID_i \| x_s)$을 획득할 수 있다. 그리고 공격자 U_a는 정당한 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 $\{ID_i, W_{ia}, C_{ia}, T_a\}$를 생성하여 원격 시스템 S에게 보냄으로서 정당한 사용자 U_i로 위장할 수 있다. 또한 $h(ID_i \| x_s)$를 불법적으로 획득한 공격자 U_a는 원격 시스템 S의 인증 메시지 $\{W_{sa}, C_{sa}, T_a''\}$를 생성하여 정당한 사용자 U_i에게 보냄으로서 합법적인 원격 시스템으로 위장할 수 있다.

따라서, An의 인증 스킴은 오프라인 패스워드 추측공격과 위장공격에 취약하다. An이 제안한 인증 스킴의 특징을 유지하면서 패스워드 추측공격, 위장공격과 재전송 공격에 대응할 수 있는 개선된 스킴을 제안한다.

3. 개선된 인증 스킴

An은 Wang-Li에 의해 제안된 스마트카드를 이용한 사용자 인증 스킴이 오프라인 패스워드 추측공격에 취약함을 보였다. 그러나 An의 인증 스킴 역시 오프라인 패스워드 추측공격에 취약하다. 따라서 개선된 인증 스킴을 제안한다.

3.1 등록단계

이 단계는 사용자 U_i가 원격시스템에 등록을 할 때 수행되며, 사용자 U_i는 자신의 아이디 ID_i와 패스워드 PW_i를 선택하고 안전한 채널을 이용하여 원격시스템에 제출하고, 다음 단계들을 수행한다.

1) 원격시스템은 h(), p, q, g 등을 선택한다. 여기서 p는 1024비트 크기를 갖는 큰 소수이고, q는 160비트 크기를 갖는 p-1의 소수 약수이다. 그리고 g는 유한체 GF(p)상에서 위수가 q인 원소이다. 또한 h()의 출력 비트 크기는 $|q|$이다.
2) 사용자 U_i의 등록 요청을 수신한 원격시스템은 다음을 계산한다.
$$R_i=h(ID_i \| x_s) \oplus h(PW_i \| x_s),$$
$$X_i=R_i \oplus h(ID_i \| PW_i)$$
여기서, x_s는 서버의 비밀키이다.
3) 원격시스템은 개별 정보 $\{ID_i, X_i, h(), p, g\}$를 저장한 스마트카드를 사용자 U_i에게 발급한다.

3.2 로그인단계

이 단계는 사용자 U_i가 로그인하여 원격시스템에게 인증 받으려고 할 때마다 수행된다. 사용자 U_i는 스마트카드를 카드리더기에 넣고 아이디 ID_i와 패스워드 PW_i를 입력한다. 그리고 스마트카드는 다음 단계들을 수행한다.

1) 스마트카드는 랜덤 수 $r \in Z_q^*$를 생성한다.
2) 랜덤 수를 이용하여 $t \equiv g^r \bmod p$를 계산한다.
3) 스마트카드는 다음을 계산한다.
$$V_i=X_i \oplus h(ID_i \| PW_i),$$
$$W_i=V_i \oplus t, \quad C_i=h(ID_i \oplus t \oplus T)$$
여기서, T는 스마트카드의 현재 타임스탬프이다.
4) 스마트카드는 사용자 U_i의 로그인 요청메시지 $M_1=\{ID_i, W_i, C_i, T\}$를 원격시스템에게 전송한다.

3.3 인증단계

인증요청 메시지 $M_1=\{ID_i, W_i, C_i, T\}$를 수신한 원격시스템과 스마트카드는 사용자와 원격시스템 사이의 상호인증을 위해 다음 과정을 수행한다.

1) 원격시스템은 사용자 U_i의 아이디 ID_i를 검증한다. 만약 형식이 유효하지 않으면 원격시스템은 사용자의 로그인 요청을 거절한다,
2) 원격시스템은 T와 T'(시스템이 C_i을 수신한 시간)사이에 시간 간격의 유효성을 검증한다. 만약 $(T'-T) \leq \triangle T$라면 원격시스템은 로그인 요청을 승인한다. 여기서, $\triangle T$는 유효한 전송 시간이다.
3) 원격시스템은 C_i'를 계산하고 C_i'과 수신한 C_i를 비교한다. 만약 비교 값이 같으면 원격시스템은 사용자 U_i를 인증하고 다음 단계를 수행한다.
$$t'=W_i \oplus h(ID_i \| x_s) \oplus h(PW_i \| x_s),$$
$$C_i'=h(ID_i \oplus t' \oplus T)$$
4) 원격시스템은 랜덤 수 $s \in Z_q^*$를 생성하고, 세션키 $K \equiv t^s \bmod p$를 계산한다.
5) 원격시스템은 다음 수식을 계산하고 사용자 U_i에게 메시지 $M_2=\{W_s, C_s, T''\}$를 전송한다.
$$u \equiv g^s \bmod p,$$
$$W_s=h(ID_i \| x_s) \oplus h(PW_i \| x_s) \oplus u,$$
$$C_s=h(ID_i \oplus u \oplus T'')$$
여기서, T''는 현재 원격시스템의 타임스탬프이다.
6) 메시지 $\{W_s, C_s, T''\}$를 수신한 스마트카드는 T''와 현재 타임스탬프 T'''간 시간 간격의 유효성을 검증한 후, 다음 수식을 계산한다.
$$u'=W_s \oplus V_i, \; C_s'=h(ID_i \oplus u' \oplus T''')$$

만약, $C_s=C_s'$이면 상호인증을 성공적으로 완성한다. 그리고, 사용자 U_i와 원격시스템 사이의 세션키 $K \equiv g^{rs} \bmod p$를 계산한다. 따라서, 원격시스템과 사용자는 상호를 인증한다.

4. 스킴 분석

본 장에서는 An의 인증 스킴을 개선한 인증 스킴에 대

하여 오프라인 패스워드 추측공격, 위장공격, 재전송공격, 그리고 순방향 비밀성에 대하여 안전성과 효율성을 분석하였다.

4.1 패스워드 추측공격

패스워드 추측공격(password guessing attack)은 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. 즉, 공격자 U_a가 패스워드를 획득할 수 있는 방법은 정당한 사용자 U_i의 스마트카드에 일시적으로 접근하여 스마트카드에 저장된 정보를 추출하고 정당한 사용자 U_i의 메시지를 도청함으로서 오프라인 패스워드 추측공격을 수행하는 것이다. 공격자 U_a는 정당한 사용자 U_i가 원격시스템 S에 로그인 요청메시지 M_1={ ID_i, W_i, C_i, T}과 원격시스템 S이 정당한 사용자 U_i에게 전송하는 메시지 M_2={W_s, C_s, T"}, 그리고 스마트카드안에 저장된 정보 {ID_i, X_i, h(), p, g}로부터 패스워드를 추측하는 것이다. 공격자 U_a는 다음과 같은 과정으로 정당한 사용자 U_i의 패스워드 PW_i를 알아내고자 할 것이다.

1 : 공격자 U_a는 정당한 사용자 U_i의 로그인 요청 메시지 M_1={ID_i, W_i, C_i, T}를 불법 획득한다.

2 : 이때 공격자 U_a는 정당한 사용자 U_i의 로그인 요청 메시지 M_1={ID_i, W_i, C_i, T}를 가로채서 W_i과 C_i를 획득한다.

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

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

(2) 공격자 U_a는 스마트카드로부터 추출한 정보 X_i과 PW_i'로부터 $W_i(=V_i \oplus t=X_i \oplus h(ID_i \| PW_i) \oplus t)$를 계산한다.

공격자 U_a는 위와 같은 방법을 시도하려고 할 것이다. 그러나 패스워드 PW_i'를 추측하는 것은 랜덤 수 $t \equiv g^r \bmod p$와 원격시스템 S의 비밀키 x_s을 알 수 없기 때문에 패스워드를 추출하는 것은 불가능하다. 따라서 제안한 인증 스킴은 오프라인 패스워드 추측공격이 불가능하다.

4.2 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 정당한 사용자 U_i로 위장하기 위해서 위조된 로그인 요청메시지 M_1={ID_i, W_{ia}, C_{ia}, T_a}를 원격시스템 S에게 보냄으로써 정당한 사용자 U_i로 위장할 수 있다. 공격자 U_a는 로그인 단계에서 가로챈 메시지 M_1={ID_i, W_{ia}, C_{ia}, T_a}로부터 원격 시스템 S의 비밀키 x_s를 얻을 수 있는 방법이 없기 때문에 서버에 성공적으로 로그인을 할 수 없다. 따라서 정당한 사용자로 위장할 수 없다. 다음은 서버 위장 공격에 대하여 분석한다. 정당한 사용자 U_i가 서버를 인증하기 위해, 원격시스템 S은 정당한 사용자 U_i에게 인증요청 메시지 M_2={W_s, C_s, T"}를 전송한다. 이때, 공격자 U_a는 정당한 사용자 U_i에게 보내는 메시지 M_2={W_s, C_s, T"}를 가로채어 원격시스템 S으로 위장하려고 할 것이다. 그러나 공격자 U_a는 $u \equiv g^s \bmod p$, 비밀키 x_s등의 정보를 얻을 수 없기 때문에 원격시스템 S로 위장 할 수 없다. 그러므로 원격시스템 S로 위장 할 수 없다. 따라서, 제안한 스킴에서는 공격자 U_a는 사용자/원격시스템으로 위장공격이 불가능하다.

4.3 재전송공격

정당한 사용자 A와 B가 원격 시스템으로부터 인증을 받은 올바른 사용자라고 가정하자. 재전송 공격(replay attack)은 이전의 정당한 사용자 A와 B사이의 정상적인 프로토콜에서 전송되었던 정보를 공격자 U_a가 가지고 있다가 나중에 사용자 A 또는 사용자 B에게 다시 보내서 프로토콜을 진행하려고 하는 공격이다.

본 논문에서 제안한 인증 스킴은 매 세션마다 스마트카드의 랜덤 수 r를 이용하여 $t \equiv g^r \bmod p$를 계산한 값, 원격 시스템의 랜덤 수 s를 이용하여 $u \equiv g^s \bmod p$를 계산한 값, 그리고 스마트카드와 원격시스템의 타임스탬프(T, T")를 생성하기 때문에 재전송 공격을 시도하려는 공격자 U_a는 $C_i'=h(ID_i \oplus t' \oplus T)$과 $C_s'=h(ID_i \oplus u' \oplus T'')$에서 C_i'와 C_s'를 얻을 수가 없다. 따라서, 이전 세션의 메시지 정보 M_1={ID_i, W_i, C_i, T}와 M_2={W_s, C_s, T"}를 이용한 재전송 공격은 불가능하다.

4.4 순방향 비밀성

정당한 사용자 U_i가 원격시스템 S로부터 인증을 받은 올바른 사용자라고 하자. 공격자 U_a가 정당한 사용자 U_i의 개인키나 패스워드를 알아냈다고 해도 이전에 정당한 사용자 U_i가 사용했던 어떠한 세션의 키도 알 수 없는 경우에 순방향 비밀성(forward security)를 만족한다고 한다.

본 논문에서는 인증단계에서 상호 교환되는 세션키 $K \equiv g^{rs} \bmod p$를 유추하는 것은 계산적으로 불가능하고, 공

격자 U_a는 정당한 사용자 U_i의 패스워드를 알아내고 스마트카드를 획득했다고 해도 각 세션의 키를 생성할 경우에는 스마트카드의 랜덤 수 $r \in Z_q^*$, 원격시스템의 랜덤 수 $s \in Z_q^*$를 사용하게 되므로 이전의 어떠한 세션에서 대해서도 사용된 키의 정보를 얻을 수 있는 방법이 없다. 따라서 이전의 세션에서 사용된 키를 알아내려면 공격자 U_a는 CDH문제를 풀어야 한다. 그러므로 제안된 인증 스킴은 순방향 비밀성을 갖는다.

4.5 비교 분석

본 절에서는 제안한 인증 스킴과 Wang-Li 및 An의 인증 스킴과 비교 분석하였다. 본 논문에서는 제안한 인증 스킴의 안전성을 분석하기 위하여 안전성 위협 요소 및 안전성 향상 요소들을 비교 분석하였다. 표 1에서 비교된 바와 같이, Wang-Li 및 An의 인증 스킴은 일부 공격에 취약함을 알 수 있고, 본 논문에서 제안한 인증 스킴은 보안 취약점에 강하다는 것을 알 수 있다.

[표 1] 안전성 분석
[Table 1] Analysis of security

스킴	패스워드 추측공격	위장공격	재전송공격	순방향 비밀성
Wang-Li	가능	가능	불가능	가능
An	가능	가능	불가능	가능
제안 스킴	불가능	불가능	불가능	가능

본 논문에서 제안한 인증 스킴은 모든 단계, 즉 등록단계, 로그인단계, 그리고 인증단계에 대한 계산량 정도는 An등의 인증 스킴과 비교할 때 유사하다. 그러나 안전성 분석에서는 보안 취약점들을 해결하여 상대적으로 효율적이라 할 수 있다. 그리고 계산 복잡도는 제안한 스킴과 An의 스킴 모두 exclusive-OR 연산을 사용하고 있다. exclusive-OR 연산은 매우 작은 계산시간이 요구되기 때문에 그 계산은 무시할 수 있다.

5. 결론

An은 Wang-Li등이 제안한 인증 스킴이 패스워드 추측공격 및 위장공격에 취약함을 보이고 이를 개선한 인증 스킴을 제안하였다. 본 논문에서는 An이 개선한 인증 스킴 역시 패스워드 추측공격 및 위장공격에 취약함을 보였고 An에 의해 제안된 인증 스킴의 특징을 유지하면서 보안 취약점들을 개선한 스마트카드 기반 인증 스킴을 제안하였다. 스마트카드를 이용한 사용자 인증 스킴에 대하여 공격자가 스마트카드에 저장된 정보를 취득함으로써 패스워드 추측공격이 가능하고 이와 함께 합법적인 사용자로 가장할 수 있다. 스마트카드 기반 인증 스킴에서 고려되는 보안 취약점들을 해결하기위해서 해시함수와 ElGamal 서명 기반의 개선된 인증 스킴은 패스워드 추측공격, 위장공격, 그리고 재전송 공격등 다양한 공격을 방어할 수 있고 또한 순방향 비밀성 기능을 제공한다. 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] M. S. Hwang, L .H. Li, "A New remote user authentication schemes using smart card," IEEE Trans. Consum. Electronics, 46(1), Feb. 2000.

[4] J .J. Shen, C. W. Cheng, and M. S Whang, "A modified remote user authentication schemes using smart card," IEEE Trans. Consum. Electron, 46(2), pp. 414-416. 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, Z. Q. Li, "A Forward-secure User Authentication scheme with smart cards," International Journal of Network Security, Vol. 3, No. 2, pp. 116- 119. 2006.

[7] Young-Hwa. An, “A Study on the user Authentication Scheme with Forward Secrecy”, Journal of the Korea Society of Computer and Information, Vol. 16, No. 2, pp. 183-191, 2011.

[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