스마트 카드를 이용한 원격 사용자 인증 방안

*유 종 상, **신 인 철
*동서울대학 전자계산과, **단국대학교 전자공학부

전화 : 031-720-2096 / 핸드폰 : 019-332-9500

A Remote User Authentication Scheme Using Smart Cards

Jong-Sang YU, In-Chul SIN
Dept. of Computer Science, DongSeoul College
E-mail : jsyoo@haksan.dsc.ac.kr

Abstract

Recently Hwang and Li[1] proposed a remote user authentication scheme using smart cards. Their scheme is based on the ElGamal public key cryptosystem and does not need to maintain a password table for verifying the legitimacy of the login users. In this paper, we proposed an advanced user authentication scheme using smart cards. Unlike Hwang and Li's scheme, smart card contains a pair of public parameters(h, P), where h is a hash function which is used in login phase. In result, we reduce one exponential computation frequency in login phase and two exponential computation frequencies in authentication phase with comparing the Hwang and Li's scheme. The proposed scheme not only provides the advantages as security of Hwang and Li's scheme, but also reduces computation cost.

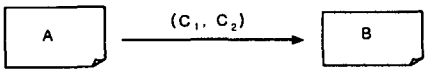
I. 서론

인터넷과 통신 시스템의 발달로 언제 어디서 누구나 정보를 공유할 수 있는 환경이 실현되고 있다. 그러나 자원의 공유에 따른 개인 사생활 침해가 심각하며, 기업의 정보 유출은 해당 기업의 자산관리에 심각한 타격을 주고 있다. 최근 이러한 문제를 해결하는 방안으로 스마트 카드를 이용한 원격 사용자의 인증 방안[1][2]들이 제안되고 있다. Wu[2]의 스마트 카드를 이용한 원격 사용자 인증 방안은 기하학적 속성에 기초한 알고리즘으로 기존에 제안되었던 계산하기 힘든 지수 계산에 기초했던 인증 방안과 비교하면 계산이 간단하고 효율적인 방안이었으나 안정성에 문제가 있다[3]. 2000년, ElGamal 공개키 암호 알고리즘에 기초한 원격 사용자 인증 방안을 Hwang, Li가 제안하였다. 본 논문에서는 Hwang, Li가 제안한 방안과 달리, 공개 변수(h, P)가 스마트 카드에 내장되어 있으며 h는 해쉬 함수이다. 해쉬 함수는 로그인 단계에서 사용되며 그들이 제안한 방안보다 계산 횟수가 적다. 그리

고 제안한 방안도 Hwang, Li의 방안과 같이 인증센터에서 패스워드 테이블 관리가 필요 없는 원격 인증 방안을 제안한다.

II. Hwang and Li의 방안

Hwang, Li는 스마트 카드를 이용한 원격 인증 방안을 제안했다. 이 방안은 ElGamal 공개키 암호 알고리즘을 기반으로 한 암호 시스템이며 ElGamal 공개키 암호 시스템은 큰 소수(P)와 유한체($GF(P)$)의 원시 원소(g)에 기초하고 있으며 인증센터에서 패스워드 테이블 관리가 필요없는 특징이 있다. 그림 1과 같이, 사용자A가 공개키(y_b)를 이용하여 메시지(M)을 암호화하여 B에 전송하면 B는 자신의 비밀키(x_b)를 이용하여 암호를 해독한다.



(그림 1) ElGamal 암호시스템

1. A는 랜덤 변수 r을 선택하여 C_1을 계산한다.

$$C_1 = g^r \bmod P$$

2. A는 B의 공개키(y_b)를 사용하여 메시지(M)을 암호화한다.

$$C_2 = M\,(y_b)^r \bmod P$$

3. A가 (C_1, C_2)을 B에게 전송한다.

4. B는 아래와 같이 평문을 계산한다.

$$M = C_2(C_1^{x_b})^{-1} \bmod P$$

Hwang, Li는 ElGamal 공개키 암호 체계와 이산대수 문제를 기반으로 인증 방안을 제안하였다. 그리고 스마트 카드를 사용한 이 방안은 가입자등록 단계, 로그인 단계, 인증 단계로 구성되어 있다.

[가입자 등록 단계]

새로운 가입자가 ID를 가입자 등록 센터에 제출하면 가입자 등록 시스템에서는 패스워드(PW_i)를 아래와 같이 계산하여 사용자에게 알려 주며 x_s는 비밀키로 시스템에서 보관한다.

$$PW_i = ID_i^{x_s} \bmod P$$

[로그인 단계]

사용자의 로그인 방법은 원격 시스템에서 입력 장치에 스마트 카드를 입력시키고 ID_i와 PW_i를 각각 키인한다. 그러면 스마트 카드는 원격 사용자를 인증할 수 있는 공개 변수 (C_1, C_2)를 연산한다. 공개 변수 연산은 다음과 같이 수행한다.

1. $C_1 = ID_i^r \bmod P$

2. $M = ID_i^{f(T \oplus PW_i)} \bmod P$

3. $C_2 = M(PW_i)^r \bmod P$

계산된 메시지 $C = (ID_i, C_1, C_2, T)$는 사용자 인증 시스템으로 전송된다.

[인증 단계]

원격 시스템으로부터 메시지 C를 받은 사용자 인증 시스템은 각 공개 변수로 다음 식의 성립 여부를 조사하여 정당한 사용자인가의 여부를 판단한다.

$$C_2(C_1^{x_s})^{-1} \bmod P = (ID_i)^{f(T \oplus PW_i)}$$

III 원격 사용자 인증 방안 제안

Hwang , Li가 제안한 스마트 카드를 이용한 원격 사용자 인증 방안을 원래의 장점을 그대로 유지하면서 계산시간을 개선하여 제안한다. 제안하는 원격 사용자 인증 절차는 다음과 같다.

[가입자 등록 단계]

새로운 가입자가 ID를 가입자 등록 센터에 제출하면 가입자 등록 시스템에서는 패스워드(PW_i)를 아래와 같이 계산한다.

$$PW_i = ID_i^{-x_s} \bmod P$$

그리고 가입자 등록 센터에서는 공개 매개변수 (h, P)을 내장한 스마트 카드를 가입자에게 제공한다. 매개 변수 P 는 이산대수에서 계산하기 어려운 1024비트 이상의 큰 소수이고 h는 해쉬함수이다.

새로운 사용자가 ID_i을 제출하면 시스템에서는 PW_i를 계산하여 비밀 통로를 통하여 가입자에게 전달한다. x_s는 시스템에서 관리하는 비밀키이다.

[로그인 단계]

사용자의 로그인 방법은 원격 시스템에서 입력 장치에 스마트 카드를 입력시키고 ID_i와 PW_i을 각각 입력한다. 그러고 스마트 카드는 원격 사용자를 인증할 수 있는 공개변수 (C_1, C_2)을 아래와 같이 계산한다.

1. $C_1 = ID_i^r \bmod P$ (r : 랜덤 변수)

2. $M = h(T \oplus PW_i) \bmod P$

   T는 스마트 카드 입력 시점의 날자와 시간이며, 인증을 위한 타임 스탬프이다. 그리고 h는 해쉬함수이다.

3. $C_2 = M\,(PW_i)^r \bmod P$

원격 시스템에서 $C = (ID_i, C_1, C_2, T)$을 사용자 인증 시스템에 전송한다.

[인증 단계]

원격 시스템으로부터 메시지 C을 받은 사용자 인증 시스템은 각 공개 변수를 검증하여 정당한 사용자 여부를 판단한다.

1. ID_i 를 검증하여 틀리면 시스템 접근을 거부한다.

2. 원격 시스템에서 보낸 시간과 인증 시스템의 시간의 간격을 다음과 같이 검사한다.

   $(T' - T) \geq \Delta T$

   ΔT가 크면 전송 시간이 오래 걸린 것으로 시스템 침입으로 간주하여 시스템 접근을 거부한다.

3. $C_2(C_1^{x_s}) \bmod P = h(T \oplus PW_i) \bmod P$ 이면, 시스템에서 사용자 로그인을 허락하고 그렇지 않으면 접근을 거부한다.

Ⅳ. 안전성 분석과 효율성

제안한 방안의 안전성을 분석하면 다음과 같다.

1. 원격 시스템에서 생성한 메시지를 도용하여 시스템을 재공격(Replaying attacks)하여도 인증 단계의 2단계에서 메시지 전송 시간(ΔT)을 점검하기 때문에 안전하다. 침입자는 시스템에 침입자는 접근할 수 없다.

2. 타임스탬프 T을 T'_a 로 변경하여 공격하여 침입하여도 로그인 3단계 $M = h(T \oplus PW_i) \bmod P$의 계산이 같지 않기 때문에 침입할 수 없다.

3. 그리고 공개 변수 $C = (ID_i, C_1, C_2, T)$은 패스워드로부터 생성되고 해쉬 함수를 사용하기 때문에 위조할 수 없다.

제안한 방안은 패스워드 테이블 관리가 필요 없고 Hwang , Li의 연구와 같은 특징을 가지며 Hwang, Li의 방안을 다음과 같이 계산량 측면에서 개선하였다.

가입자 등록 단계에서 패스워드는 오프라인 상태에서 계산되며 가입자에게 스마트 카드와 함께 전달된다. 패스워드는 로그인 단계와 인증 단계에서 온라인 상태로 사용자의 필요에 따라 사용된다. 따라서 패스워드 발급시, 계산 방법과 인증 방법을 개선할 수 있다.

패스워드 발급시 계산 : $PW_i = ID_i^{-x_s} \bmod P$

인증시 계산 : $C_2(C_1^{x_s}) \bmod P$

Hwang, Li는 $M = ID_i^{f(T \oplus PW_i)} \bmod P$ 을 사용하였으나, 제안한 방안에서는 해쉬 함수를 이용하여 다음과 같이 개선하였다.

$$M = h(T \oplus PW_i) \bmod P$$

온라인 상태에서 스마트카드의 계산능력과 사용자의 편리성 문제를 개선하기 위해 안전성 있는 해쉬 함수

만을 적용한다.

Hwang, Li의 방안과 제안한 방안의 계산량 측면에서의 효율성 분석을 하면 표 1과 같다.

표 1. 두 방안의 효율성 분석표

구분	Hwang-Li 방안	제안 방안
로그인 단계	· 지수계산 3회 · 해쉬함수 1회	· 지수계산 2회 · 해쉬함수 1회
인증 단계	· 지수계산 4회 · 해쉬함수 1회	· 지수계산 2회 · 해쉬함수 1회

V. 결론

ID와 패스워드를 이용한 원격 사용자 인증에서 패스워드의 비밀 유지와 사용자 인증 계산 방법은 중요한 기술이다. 본 논문에서는 패스워드, 로그인과 인증 단계 계산 방법을 개선하였다. 가입자 등록 단계에서 패스워드가 발급된 이후, 사용자가 시스템을 이용할 때마다 사용자 인증이 필요함으로 패스워드 발급과 연관하여 인증 단계의 계산 방법을 개선하였다. 로그인 단계에서 해쉬 함수를 사용함으로써 Hwang, Li의 방안과 비교하여 계산 횟수가 적으므로, 보다 실용적인 방안을 평가된다.

참고문헌

[1] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transaction on Consumer Electronics, Vol. 46, No 1., 2000, pp. 28-30.

[2] T.C. Wu, "Remote login authentication scheme based on a geometric approach", Compt. Commun. Vol. 18, No 1., 1995, pp. 959-963.

[3] T. ElGamal, "A public-key cryptosystem and scheme based on discrete logarithms," IEEE Transaction on Information Theory Vol 31, 1995, pp. 469-472.

[4] T. Hwang, Y, Chen, and C.S. Laih, "Non-interactive password authentications without password tables," IEEE Region 10 Conforence on Computer and Communication System, IEEE Computer Society, 1990, pp. 429-431.

[5] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," International Journal Of Computer Mathematics, 1999, pp. 657-666.

[6] L. Lamport, "Password authentication with insecure communication," Communications of ACM, Vol.24, 1981, pp.770-772.

[7] C.C. Chang and L.H. Wu, "A password authentication scheme based upon Rabin's public-key cryptosystem," Proceedings of the International Conference on Systems Management, Hong Kong, 1990, pp.425-429.

[8] C.H. Lin, C.C. Chang, T.C. Wu and R.C.T. Lee, "Password authentication using Newton's in interpolating polynomials," Information Systems, Vol. 16, No 1, 1991. pp.97-102.

[9] Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security: Private communication in a public world," Prince Hall, 1995.