스마트 카드를 이용한 ID기반의 키 교환 프로토콜

배헌중[0] 김현성[00] 유기영[0]
[0]경북대학교 컴퓨터공학과, [00]경일대학교 컴퓨터공학과
{tonybae99[0], yook[0]}@infosec.knu.ac.kr, [00]kim@kiu.ac.kr

ID-based Key Exchange Protocol using Smart cards

Hun-Joong Bae[0] Hyun-Sung Kim[00] Kee-Young Yoo[0]
[0]Dept. of Computer Engineering, Kyungpook National University
[00]Dept. of Computer Engineering, Kyungil University

요 약

본 논문에서는 사용자의 식별 정보를 이용하여 두 시스템간에 인증과 키 교환을 스마트 카드를 이용하여 수행하는 ID기반의 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 사용자의 스마트 카드와 입력 지문 특징점 정보를 이용하여 스마트 카드와 시스템간에 세션키를 교환한다. 제안한 프로토콜의 안전성은 이산 대수 문제와 Diffie-Hellman 문제의 어려움에 기반하며 완전한 전 방향 보안을 제공하고 가장 공격, 잠재적인 재전송 공격을 방지할 수 있다.

1. 서론

ID기반의 프로토콜은 비밀키나 공개키들의 교환이 필요 없고 공개키 디렉토리 테이블이 필요하지 않으며 중재자의 도움이 필요하지 않다는 장점들이 있다. ID 기반 시스템 개념은 Shamir에 의해서 처음으로 제안되었다[1]. Shamir는 사용자 식별 정보 이용으로 파일 저장소를 배제한 암호 시스템과 서명 프로토콜을 제안하였다. ID 기반 시스템은 사용자 식별 정보를 유일하게 확인할 수 있는 이름, 주민등록 번호 등 사용자의 식별 정보만으로도 상대방을 인증할 수 있고 이것을 바탕으로 공개키 기반의 전자서명과 키 분배를 사용자간에 독립적으로 할 수 있다.

키 분배를 위해서 Diffie-Hellman은 간단한 프로토콜을 제안하였다[2]. Diffie-Hellman의 키 교환 프로토콜은 두 사용자간 또는, 두 시스템간에 공통된 세션키를 공유하기 위한 목적으로 사용된다. Diffie-Hellman 키 교환 프로토콜의 안전성은 이산 대수 문제의 어려움에 그 기반을 두고 있다.

Okamoto의 ID기반 프로토콜은 Shamir의 생각을 확장하여 RSA 공개키 암호 시스템에 기반을 두고 키 분배와 디지털 서명을 조합하였다[4]. 이 프로토콜의 안전성은 두 개의 큰 소수의 곱인 합성수의 인수분해 문제에 기반한다. 그러나, 많은 대역폭의 사용과 많은 계산량이 요구된다. 또한, 가장 공격 등 안전성에 문제점이 있다.

본 논문에서는 사용자 식별 정보를 이용하여 스마트 카드를 이용한 ID기반의 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 ElGamal 공개키 암호 시스템을 기반으로 하고, Diffie-Hellman의 키 교환 방식과 입력지문 정보를 이용한다. 인증 및 키 교환 단계에서 스마트 카드와 입력 지문 특징점 정보를 이용하여 두 시스템간의 세션키를 교환한다. 제안한 프로토콜의 안전성은 이산 대수 문제와 Diffie-Hellman 문제의 어려움에 기반하며 완전한 전방향 보안(Perfect forward secrecy)을 제공하고 가장 공격 방지(Impersonation attack), 잠재적인 재전송 공격(Potential replay attack)을 방지할 수 있다.

2. 배경 지식

2.1 지문 검증

본 논문의 지문 검증 방법은 특징점 추출(Minutia extraction)과 매칭(Matching)을 기반으로 한다[5][6]. 특징점 추출이란 지문 영상에서 단점(Ending)과 분기점(Bifurcation)의 위치를 찾는 과정을 말하며 개인의 지문에서 추출된 특징점을 실질적인 신분 확인을 위해 등록된 특징점과 비교하여 같은 손가락에서 찍힌 지문인지를 판단하는 것을 매칭이라 한다. 특징점 기반의 일반적인 매칭 방법은 특징점 간의 기하학적으로 구성된 그래프 패턴의 비교로 이루어진다. 두 지문의 일치 여부는 정합도(Matching score)로 산출되며, 산출된 정합도가 적정 기준을 결정하게 된다. 일반적으로 지문 인식 시스템들은 정합도의 문턱 값(Threshold)을 조절함으로서 그 보안 수준을 결정하게 된다. 지문은 사용자의 고유성과 평생 불변성으로 입력 될 때마다 다른 특징점 지도(Minutia map)가 만들어지고, 이 특징점들이 x축과 y축, 방향각(θ)값을 가지는 좌표값들을 이용하므로 추정이 불가능하다. 그러므로, 생성된 지도를 이용하여 원 타임 난수(One-time random number)를 생성할 수 있다. 이 난수는 개인키와 동일한 역할을 하므로 매우 중요하다. 만약 같은 난수가 한번 이상 사용된다면, 공격자는 난수와 개인키 등을 이용하여 선택된 난수와 개인키를 획득할 수 있다. 원 타임 난수를 생성하는 것은 제안한 프로토콜에

서 아주 중요하다.

2.2 등록 단계

시스템 파라미터는 다음과 같다. p는 큰 소수(Large prime number)이고 1024비트의 크기로 가정한다. f는 일 방향 함수(One-way function)이며 g는 원시 근(Primitive root)이다. 이들 값은 공개한다. U_i는 합법적인 사용자 i, PW는 사용자의 패스워드, ID_i는 U_i의 식별자이고 CID_i는 U_i의 스마트 카드 식별자이다. U_i는 지문 특징점 매칭으로 소유자 인증을 할 수 있는 스마트 카드를 소유한다[6]. 각 사용자는 지문을 사용하여 스마트 카드의 소유자임을 증명한다. 그러므로, 스마트 카드의 소유자만이 스마트 카드에 접근할 수 있다. 본 논문의 프로토콜을 강화하기 위해서 스마트 카드에 프로토콜의 수행에 필요한 모든 값을 저장한다.

사용자 U_i가 등록을 위해 시스템에게 ID_i을 보낸다. 시스템은 다음과 같이 사용자의 패스워드를 계산한다[7].

(1) $ID'_i=(ID_i)^{SK_1} \bmod p$,

(2) $PW_i=(ID'_i)^{SK_2} \bmod p$,

(3) U_i의 스마트 카드 식별자(CID_i)를 생성한다.

여기서 SK_1과 SK_2는 시스템이 유지하는 비밀 키들이고 CID_i는 검증 단계에서 등록된 스마트 카드인지 여부를 확인하기 위해 이용된다. 이 단계가 끝나면 시스템은 스마트 카드에 공개 인자들 (f,p,g) 과 CID_i와 PW를 저장하고, 스마트 카드를 안전한 방법으로 U_i에게 전달한다.

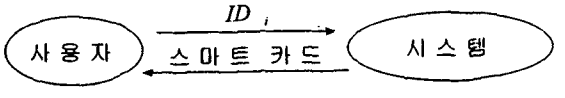

그림1 등록 단계

(1) 사용자 -> 시스템 : ID_i

(2) 시스템 -> 사용자 : 스마트 카드(CID_i, f, p, g, PW)

3. 인증 및 키 교환 프로토콜

3.1 인증 및 키 교환 단계

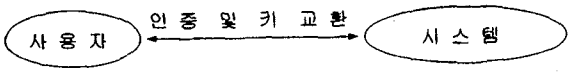

그림2 인증 및 키 교환 단계

U_i는 시스템에 인증하기 위해서 터미널에 스마트 카드를 넣고, ID_i를 입력한다. 그리고 지문 입력 장치 상에 U_i의 지문을 찍는다. 만약 U_i의 지문이 스마트 카드에 의해서 성공적으로 소유자 인증이 수행되면[6]스마트 카드와 시스템은 다음과 같은 연산을 수행한다.

(1) U_i의 패스워드를 이용하여 $P_i=g^{PW_i}$를 계산하고 입력 지문의 특징점 좌표값들을 이용하여 난수(r)을 생성한다. 스마트 카드는 인증을 위해서 다음과 같이 계산한다.

$X_i=(g)^r$,

$Y_i=ID_i(P_i)^r$,

시스템에게 인증 메시지 $M_1=\{ID_i,CID_i,X_i,Y_i\}$ 를 보낸다.

(2) 인증 메시지 $M_1=\{ID_i,CID_i,X_i,Y_i\}$ 를 받은 시스템은 ID_i와 CID_i의 유효성을 확인한다. 만약, 이들 중 어느 하나도 유효하지 않다면 인증은 거부되고 연결은 끊어진다. 시스템은 등식 $Y_i(X_i^{PW_i})^{-1}=ID_i$ 의 성립을 확인한다. 만약 성립되지 않다면, 인증은 거부되고 연결은 종료된다. 인증이 성공하면, 시스템은 검증 단계를 위해 ID_i와 CID_i을 저장해 두고, 세션 난수 $N=f(CID_i,rj)$ 을 계산하고 세션 난수를 이용하여 다음과 같이 계산한다.

$X_j=(g)^{rj}$,

$Y_j=N(X_i)^{rj}$,

시스템은 인증 메시지 $M_2=\{N,X_j,Y_j\}$ 를 스마트 카드에게 전송한다. 여기서, rj는 시스템의 난수 발생기에 의해 생성되는 난수이고 f는 일 방향 함수이다.

(3) 인증 메시지 $M_2=\{N,X_j,Y_j\}$ 를 받은 스마트 카드는 등식 $Y_j(X_j^r)^{-1}=N$ 이 성립하는지를 확인한다. 만약 성립하지 않는다면 스마트 카드는 시스템을 인증 거부한다.

(4) 스마트 카드와 시스템의 두 당사자간에 양방향 인증이 되면 세션키를 각각 $SK_i=(X_j)^r \bmod p$, $SK_j=(X_i)^{rj} \bmod p$를 계산한다. 두 당사자간에 공통된 세션키 $(g^{r\cdot rj})$를 가지고 있다는 것을 알 수 있다. 그림3 에서 사용된 SK_i는 사용자의 세션키, SK_j는 시스템의 세션키이다.

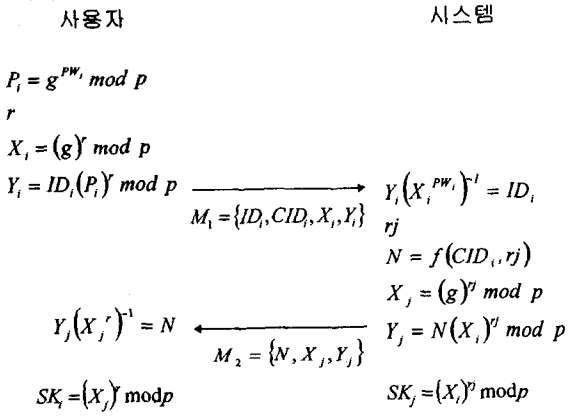

그림3 인증 및 키 교환 프로토콜

3.2 검증 단계

두 당사자간에 인증 및 키 교환을 검증하기 위해 스마

트 카드와 시스템은 인증 여부를 결정하고 세션키를 검증하기 위해 다음과 같은 단계를 수행한다.

(1) 시스템은 U_i의 ID_i와 CID_i의 유효성을 테스트하고 등식 $Y_i(X_i^{PW_i})^{-1}=ID_i$ 이 성립을 검증한다. 만약 등식이 성립되지 않는다면 시스템은 스마트 카드를 인증하지 않는다.

(2) 스마트 카드는 등식 $Y_j(X_j^r)^{-1}=N$ 이 성립하는지를 검증한다. 만약 성립되지 않는다면 스마트 카드는 시스템을 인증하지 않는다.

(3) 프로토콜에서 스마트 카드는 $SK_i=(X_j)^r \bmod p$ 을 통하여 키 검증을 하며, 시스템은 $SK_j=(X_i)^{rj} \bmod p$으로 검증한다. 이 프로토콜에서 $SK_i=SK_j=g^{r\cdot rj} \bmod p$ 이므로, 스마트 카드와 시스템 사이에 공통의 세션키가 성립된다.

두 당사자간의 인증은 합법적이고 그 인증을 의해서 생성된 인증 메시지임이 증명되기 때문에, 시스템은 스마트 카드를 인증하고 스마트 카드는 시스템을 인증한다. 동시에 공통된 세션키를 가진다.

4. 암호학적 분석

본 절에서는 제안한 프로토콜의 암호학적 분석을 위하여 세 가지 공격, 완전한 전방향 보안과 잠재적 재전송 공격 및 가장 공격, 측면에서 기술하고자 한다.

먼저, 제안한 프로토콜은 ElGamal 공개키 암호 시스템을 기반으로 하고 있기 때문에 $ID_i'=(ID_i)^{SK} \bmod p$ 와 $PW_i=(ID'_i)^{SK_2} \bmod p$의 계산으로부터 비밀키 SK_1과 SK_2를 계산하는 것은 매우 어렵다. 더욱이, 인증 및 키 교환 단계에서 $X_i=(g)^r$ 로부터 난수(r)를 유도하는 것이 어렵다. 이 어려움은 유한 필드 상에서 이산 대수의 어려움에 기인한다. 특징점 기반의 지문 검증 시스템에서, U_i가 지문을 찍을 때마다, 다른 특징점 지도가 생성된다. 따라서, 이 특징을 이용하여 원 타임 난수를 생성할 수 있다.

완전한 전방향 보안은 현재의 세션키를 공격자가 알게 되더라도 그 이전의 세션키를 추측할 수 없을 때 제공된다. 제안한 프로토콜에서 전방향 보안에 대한 공격을 위해서는 네트워크 상에서 획득 가능한 전송된 메시지 g^r과 g^{rj}로부터 $g^{r\cdot rj}$를 유추할 수 없어야 한다. 그러나, 제안한 프로토콜에서는 세션키 생성을 위해 입력 지문 정보로부터 난수값을 조합했고, 전송된 메시지 g^r과 g^{rj}로부터 $g^{r\cdot rj}$추측은 이산 대수의 어려움에 기반 한 문제이다.

재전송 공격은 인증 및 키 교환 단계에서 시스템의 메시지, $N=f(CID_i, rj)$, $X_j=(g)^{rj}$, $Y_j=N(X_i)^{rj}$에서 세션 난수(N)을 이용함으로써 잠재적인 메시지 재전송 공격을 방지할 수 있다. 공격자가 새로운 인증을 위해 이전 세션에서 획득한 인증 메시지를 재전송 한다고 가정하자. 인증 및 키 교환 단계에서, 공격자는 처음에 $M_1=\{ID_i, CID_i, X_i, Y_i\}$ 을 시스템에게 보낸다. M_1을 받은 시스템은 새로운 세션 난수(N')을 생성하고 그것을 공격자에게 보낸다. 그러면 공격자는 그 이전에 가로챈 인증 메시지(M_2)로 등식 $Y_j(X_j^r)^{-1}=N'$ 을 검증한다. 공격자는 등식 $Y_j(X_j^r)^{-1}=N'$ 이 성립되지 않으므로 인증은 실패할 것이다. 결국, 인증은 거부되고 공격은 실패할 것이다. 그러므로, 제안한 프로토콜은 잠재적인 재전송 공격에 효율적으로 대응할 수 있다. 또한, 두 시스템간의 동기화 된 시계가 제공되지 않더라도 재전송 공격에 대응하여 사용자들을 보호할 수 있다.

가장 공격은 만약 공격자가 다른 적합한 사용자로 가장할 수 있다면 공격자에 의한 공격이 가능하다. 따라서, 프로토콜은 가장 공격을 방지하기 위해 매우 중요한 중간 레이어를 제시했다. 제안한 프로토콜에서는 Lee 등이 제안한 방법과 같은 방법을 이용한다[7]. 따라서, 공격자는 다른 적합한 사용자로 가장할 수 없고, 그 결과로 제안한 프로토콜은 사용자 가장 공격에 대응할 수 있다.

5. 결론

본 논문에서는 사용자의 식별 정보를 이용하여 두 시스템간에 인증과 키 교환을 스마트 카드를 이용하여 수행하는 ID기반의 키 교환 프로토콜을 제안하였다. 제안한 프로토콜은 사용자의 스마트 카드와 입력 지문 특징점 정보를 이용하여 스마트 카드와 시스템간에 세션키를 교환하였다. 제안한 프로토콜의 안전성은 이산 대수 문제와 Diffie-Hellman 문제의 어려움에 기반하며 완전한 전방향 보안을 제공하고 가장 공격, 잠재적인 재전송 공격을 방지할 수 있다.

참 고 문 헌

[1] A. Shamir, "Identity-based cryptosystems and signature schemes", *in Proc. Crypto-84*, Santa Barbara, CA, pp. 47-53, 1984.

[2] W. Diffie, and M. E. Hellman, "New direction in cryptography", *IEEE Trans*, IT-22, pp. 644-654, 1976.

[3] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, IT-31(4), pp. 469-472, 1985.

[4] E. Okamoto, and K. Tanaka, "Identity-based information security management system for personal computer networks", *IEEE Journal on selected areas in communications*, Vol. 7, No. 2, pp. 290-294, 1989.

[5] Ratha, N. K. and Jain, A. K., "A real-time matching system for large fingerprint databases", *IEEE Trans. Pattern Anal. Mach. Intell.*, 18, pp. 799-813, 1996.

[6] Jain. A, et al, *Biometrics personal identification in networked society*, (Kluwer Academic Publishers, 1999), pp. 369-384.

[7] J. K. Lee, S. R. Ryu and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards", *Electronics letters* 6th June, Vol. 38, No. 12, pp. 554-555, 2002.