스마트카드를 이용한 ID기반의 사용자 인증 프로토콜

이원진° 김은주 전일수
금오공과대학교 전자통신공학과
{wjlee°, candycore, isjeon}@kumoh.ac.kr

ID-based User Authentication Protocol using Smartcard

Won Jin Lee° Eun Ju Kim Il Soo Jeon
Kumoh National Institute of Technology, School of Electronic Engineering

요 약

최근 김등[1]은 스마트카드와 패스워드 그리고 지문 정보를 이용한 ID 기반의 사용자 인증 프로토콜을 제시하였다. 그러나 Scott[2]은 그 프로토콜이 보안에 취약함을 보였다. 본 논문에서는 Scott이 제안한 공격에 안전할 뿐만 아니라 다양한 공격에 안전한 패스워드와 스마트카드를 이용한 ID기반의 사용자 인증 프로토콜을 제안한다.

1. 서 론

오늘날 전자상거래나 신용 거래에 있어 보안은 컴퓨터 네트워크를 위한 중요한 이슈라 할 수 있다. 사용자 인증은 원격 로그인 시스템을 위한 기본적인 보안 메커니즘이며, 이러한 개체 인증은 보안 서비스들 중 가장 중요한 서비스 중 하나이며, 통신 개체들 간의 적법성을 확인하고 검증하기 위해 필요하다.

최근 김등[1]은 스마트카드와 지문을 이용한 ID기반의 사용자 인증 프로토콜을 제안하였다. 그들의 프로토콜에서는 사용자 인증을 위하여 프로토콜 수행에 필요한 정보는 스마트카드에 저장하고 모든 연산은 스마트카드 내부에서 수행하며, 스마트카드의 소유자 인증과 난수 생성을 위하여 지문 정보를 이용하였다. 하지만 Scott[2]은 김등이 제시한 프로토콜이 보안에 취약함을 보였다. Scott의 공격을 통해서 김등의 프로토콜에서는 지문의 추가적인 사용이 인증 시스템의 안전성에 영향을 미치지 못함을 확인할 수 있다.

본 논문에서는 Scott에 의한 공격에 대한 보안의 취약점을 해결하기 위해 스마트카드와 패스워드를 이용한 ID기반의 사용자 인증 프로토콜을 제시하였다. 제시한 프로토콜은 기존의 프로토콜보다 높은 안전성과 효율성을 제공하며, 수행에 필요한 모든 정보는 스마트카드에 저장되고 모든 연산은 스마트카드 내부에서 이루어진다.

2. 관련연구

Shamir에 의해 ID(Identification)정보에 기반한 서명 기술이 제안된 이후 ID정보에 기반한 많은 연구가 진행되었다[3]. 이산대수를 이용한 영지식 대화형 프로토콜이 Chaum등[4]에 의해 제안되었고, Schnorr[5]는 여기에서 아이디어를 얻어 *mod p*상의 이산 대수 문제를 이용하여 계산능력이 약한 스마트카드에 적합한 새로운 ID방식을 제안하였다. Wang등[6]과 Yang[7]은 스마트카드를 이용한 ID기반의 인증 프로토콜을 제안하였다. 최근에 김등[1]은 스마트카드와 지문을 이용한 ID 기반의 사용자 인증 프로토콜에 대해서 제안하였다.

김등[1]이 제시한 프로토콜은 단계3로 구성된다. 원격서버가 클라이언트에게 스마트카드를 발급하고, 클라이언트는 자신의 지문 정보를 스마트카드에 등록하는 등록단계와 스마트카드와 자신의 지문을 입력하여 원격서버에 로그인 요청을 하는 로그인 단계, 마지막으로 원격서버가 로그인 요청에 대한 판단을 확인하는 검증단계로 구성되어 있으며, 그림 1에서 그 과정이 제시되어 있다.

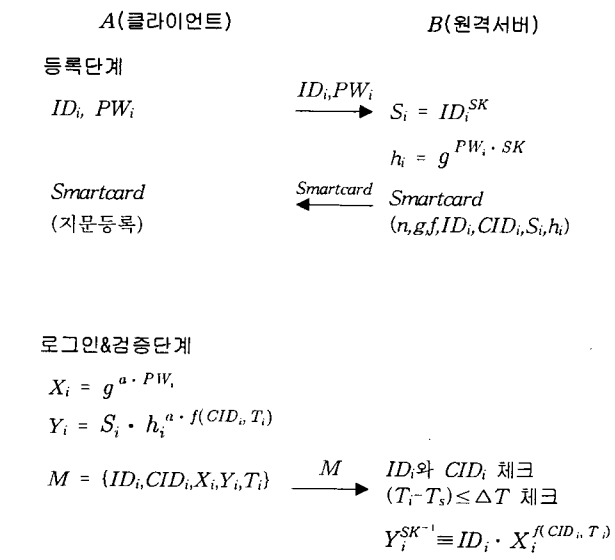

그림 1. 김등[1]의 인증 프로토콜

하지만 Scott은 그림1에서 제시한 김등의 방법에 대한

보안의 취약점을 제시하였다. 김등의 프로토콜에 대해 Scott은 지문정보에 대한 소유가 없더라도 검증 확인을 위해 통과하는 X_i와 Y_i값을 알 수 있음을 검증하였고, 소극적인 도청자에 대해서조차 안전하지 못함을 보였다. 본 논문에서는 Scott이 지적한 보안의 취약점을 해결하는 보다 효율적이고 안전한 스마트카드를 이용한 ID기반의 사용자 프로토콜에 대해서 제안한다.

3. 제안한 사용자 인증 프로토콜

본 장에서는 스마트카드를 이용하여 사용자를 인증 할 수 있는 ID기반의 인증 프로토콜을 제안한다. 제안한 프로토콜은 등록 단계와 로그인 단계, 그리고 검증 단계의 3단계로 구성된다. 먼저 등록 단계에서는 원격서버가 사용자에게 스마트카드를 발급하고, 스마트카드를 발급받은 사용자는 로그인 단계에서 자신의 패스워드를 입력하여 로그인 요청을 원격서버에게 전송한다. 검증 단계에서 원격서버는 사용자로부터 받은 메시지가 정확한지 여부를 확인하고 로그인 요청을 받아들일지를 판단한다.

3.1 표기법 정의

본 절에서는 제안된 프로토콜들에서 사용될 용어와 표기법에 대해서 먼저 살펴보고, 프로토콜의 참여자들 간에 동의해야 할 내용을 기술한다.

A, B	각각 클라이언트와 서버
ID_i	클라이언트 i의 식별자
CID_i	스마트카드의 식별자
g	곱셈군(multiplicative group) Z_n^*의 생성자(generator)
n	큰 소수
PW_i	클라이언트의 패스워드
SK	서버의 비밀키
SK^{-1}	Z_n^*상에서 SK의 역수
T_i	시스템의 현재 시스템 클럭
$f(\ )$	일방향 해쉬 함수(one-way hash function)

여기에서 클라이언트 A와 서버 B는 합법적인 참여자들로써 g와 n을 미리 공유하고 있다는 가정 하에 제안된 프로토콜을 수행한다.

3.2 제안한 프로토콜의 수행

본 논문에서 제안한 프로토콜은 등록과 로그인 단계, 그리고 검증 단계의 3단계로 구성된다.

(1) 등록단계

원격서버는 프로토콜 수행에 필요한 정보를 스마트카드에 저장하여 클라이언트에게 발급하며 그 절차는 다음과 같다.

단계1. 클라이언트 A는 자신의 ID_i와 PW_i를 원격서버 B에게 안전한 방법으로 전송한다.

단계2. 원격서버 B는 ID_i의 적법성을 체크하고 스마트카드 식별자인 CID_i를 생성하고 S_i와 h_i를 다음과 같이 계산한다.

$$S_i = ID_i^{SK} \pmod n$$
$$h_i = g^{PW_i \cdot SK} \pmod n$$

여기서 CID_i는 검증단계에서 스마트카드의 유효성 검증을 위한 것이다.

단계3. 원격서버 B는 n, g, $f(\ )$, ID_i, S_i, h_i를 스마트카드 메모리에 저장하고 스마트카드를 클라이언트 A에게 발급한다.

(2) 로그인 단계

로그인을 위해서 클라이언트 A는 발급 받은 스마트카드를 카드리더에 입력하고 소유자 인증을 수행한 후, 스마트카드는 원격서버의 로그인에 필요한 정보 ID_i와 패스워드 PW_i를 사용자에게 요청한다. 스마트카드는 다음과 같은 로그인 절차를 수행한다.

단계1. 스마트카드는 다음을 계산한다.

$$N = f(CID_i, T_i) \pmod n$$
$$X_i = g^{PW_i} \pmod n \oplus S_i$$
$$Y_i = S_i \cdot h_i^N \pmod n$$

여기서 T_i는 시스템의 현재 시스템 클럭이고, $f(x,y)$는 해쉬함수이다 .그리고 $\oplus$는 XOR 연산을 말한다.

단계2. 로그인 메시지 M을 원격서버 B에게 전송한다.

$$M = \{ID_i, CID_i, X_i Y_i, T_i\}$$

(3) 검증단계

원격서버는 클라이언트 A가 정당한 사용자인지를 검증한다. 이러한 검증을 위하여 메시지 M이 원격서버의 시스템 클럭 T_s에 도착했다고 가정하며, 그 절차는 다음과 같다.

단계1. 사용자의 유효한 아이디 ID_i와 적법한 스마트카드의 아이디 CID_i가 각각 소유자 아이디인지를 검증한다. 만약 부적법한 정보이면 로그인 요청을 거절한다.

단계2. $(T_s - T_i) \le \Delta T$ 연산에 의해서 적법한 지연 시간에 메시지가 보내졌는지를 검증한다. 여기서 ΔT 는 전송 지연을 고려한 적법한 지연시간이다. 만약 위의 조건을 만족하지 못한다면, 원격서버는 서비스 요청을 거절한다. 적법한 시간 간격은 네트워크 환경에 의해서 다양하게 조정될 수 있다.

단계3. 원격서버는 $N = f(CID_i, T_i)$과 $S_i = ID_i^{SK}$ 를 계산한 후 다음 수식의 유효성을 검증한다.

$$Y_i^{SK-1} \equiv ID_i \cdot (X_i \oplus S_i)^N$$

위 수식은 클라이언트에 의해 입력된 패스워드 PW_i가 원격서버에 의해 발급된 스마트카드에 등록된 패스워드와 일치할 때만 성립된다. 즉, 이 수식이 성립할 때만 원격서버는 클라이언트의 접근을 허락한다. 전체 단계는 그림 2와 같이 살펴볼 수 있다.

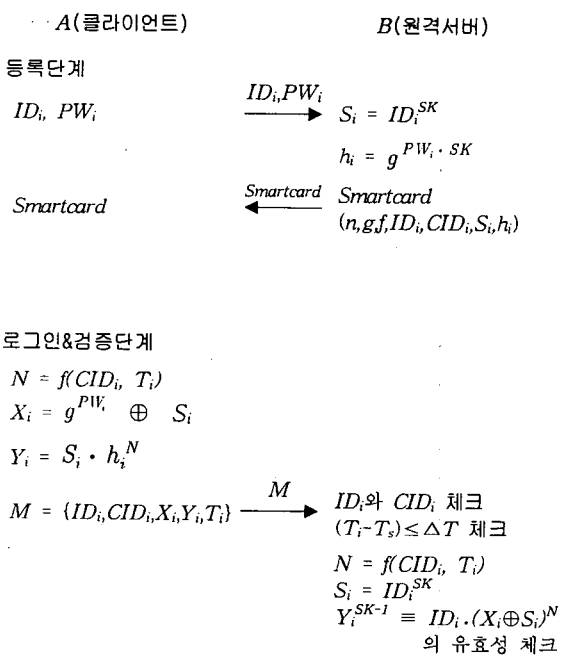

그림 2. 제안된 인증 프로토콜

4. 분석

본 논문에서 제안한 프로토콜을 패스워드 추측공격(password guessing attack), 메시지 재전송 공격(message reply attack), 그리고 위장공격(impersonation attack)의 세 가지 측면에서 안전성을 분석한다. 패스워드 인증은 사용자 인증에서 가장 널리 사용되고 있는 기법이다. 패스워드를 획득하기 위해서 공격자는 $h_i = g^{PW_i \cdot SK}$ 을 통해서만 PW_i를 추측할 수 있다. 그러나 이러한 공격은 h_i가 안전한 스마트카드에 저장되어 있어서 소유자 인증 없이는 직접적으로 h_i에 접근할 수 없기 때문에 불가능하다. 또한, 공격자가 h_i를 알더라도 패스워드 PW_i는 안전하게 유지된다. 이것은 유한필드 상의 이산대수 문제의 어려움에 근거한다.

제안한 기법은 시스템 클럭을 사용하기 때문에 메시지 재전송 공격에 안전 할 수 있다. 로그인 요청 메시지 $Y_i^{SK-1} \equiv ID_i \cdot (X_i \oplus S_i)^N$에서 시스템 클럭이 사용된다. 공격자가 메시지 재전송 공격을 위해서는 이전 세션에서 획득한 Y_i 의 시스템 클럭 T_i를 $(T_s - T_i) \le \Delta T$를 만족하는 T'로 변경할 수 있어야 한다. 그러나 이것은 불가능하며 문제역시 이산대수의 어려움에 근거하고 있다.

마지막으로 본 논문에서 제안한 기법은 위장공격에 안전하다. 적법한 사용자가 타인을 위장하기 위해서는 위장하고자 하는 사용자의 아이디와 패스워드를 알아야만 한다. 그러나 적법한 사용자의 아이디와 패스워드는 연산 $S_i = ID_i^{SK}$와 $hi = g^{PW,SK}$에 의존적이다. 위장 공격을 위해서는 두 식으로부터 원격서버의 비밀키 SK를 알아야 하지만 이 값을 찾는 것 역시 이산대수의 어려움에 근거하고 있다. 또한 논문에서 제안한 기법은 Scott이 지적한 보안의 취약점에 대해서도 안전하다. 공격자가 $M = \{ID_i, CID_i, X_i, Y_i, T_i\}$를 알고 있더라도, S_i $(=ID_i^{SK})$를 추측하거나 계산 할 수 없다. 왜냐하면 스마트카드에 S_i가 저장되어 있으며, 적법한 사용자와 원격서버만이 이 값을 알고 있기 때문이다.

5. 결론

본 논문에서는 패스워드와 스마트카드를 이용한 ID기반의 사용자 인증 프로토콜을 제안하였다. 본 논문에서 제안한 프로토콜은 Scott 등의 공격에 대항할 수 있을 뿐만 아니라 다양한 공격에 안전성과 효율성을 제공한다. 본 논문에서 제안한 프로토콜은 김등[1]이 제안한 프로토콜에서 지문 정보를 이용하는 오버헤드를 줄였으며, 그 프로토콜 결함을 해결할 수 있는 프로토콜이다.

[참고문헌]

[1] H.S.Kim, S.W.Lee, K.Y.Yoo, *ID-based Password Authentication Scheme using Smart Cards and Fingerprints*, ACM Operating Systems Review, pp. 32-41, Oct. 2003.

[2] M.Scott, *Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints*, IACR e-print archive, 2004.

[3] A.Shamir, *Identity-based cryptosystems and signature schemes*, proceedings CRUPTO'84, LNCS 196, pp. 47-53. 1984

[4] D.Chaum, J.H.Evertse and J.van de Graaf, *An improved protocol for demonstration possession of discrete logarithms and some generalizations*, Eurocrypt'87, pp. 127-141, 1987.

[5] Schnorr, *Efficient identification and signatures for smart cards*, Eurocrypt'89, pp. 686-689, 1989.

[6] S.J.Wang, J.F.Chang, *Smart card based secure authentication scheme*, Computers and Security, Vol. 15, No. 3, pp. 231-237, 1996.

[7] W.H.Yang, S.P.Shieh, *Password authentication schemes with smart cards*, Computers and Security, Vol. 18, No. 8, pp. 727-733, 199.