스마트카드를 이용한 원격 사용자 인증 프로토콜

김한수[0] 송하윤
홍익대학교 컴퓨터 공학과
{kimhs[0], song}@cs.hongik.ac.kr

A remote user authentication protocol using a Smart Card

Han-soo Kim ,Ha-yoon Song
College of Information and Computer Engineering, Hongik University

요 약

정보 기술의 급속한 발전으로 스마트카드는 무선 통신, 공중전화 서비스, 전자 상거래, 교통 분야등 여러 활용 분야에서 사용되고 있으며 특히 현금이나 신용카드를 대체하는 결제수단으로 떠오르면서 우리 생활에 많은 변화를 일으키고 있다. 그러나 이러한 편리함 뒤에는 평소 우리가 생각하지 못했던 일들, 예컨대 개인 정보의 유출 등의 사고가 발생하여 시스템 안전에 대한 문제가 재기되고 있는 실정이다. 그동안 스마트카드를 이용한 원격 인증에 있어 ElGamal 알고리즘이나 해쉬 함수를 이용하여 시스템이 사용자를 인증하는 단방향 인증이 연구되어 왔으나, 기술의 발달로 시스템에 대한 위조가 가능해지면서 보다 강화된 보안의 필요성이 대두되었다. 본 논문에서는 이산대수와 해쉬 함수를 결합한 하이브리드 방식으로 스마트카드를 이용한 원격 사용자 양방향 인증을 설계하였다.

1. 서 론

원격 인증 스킴은 보호받지 못한 통신상에서 원격 사용자를 인증하는 매카니즘이다. 1981년 Lamport [1]가 원격 인증 스킴을 제안한 이후로 안전성(security), 효율성(efficiency)면에서 향상된 여러 스킴들이 제안되었다 [2~6]. Hwang과 Li [2]는 스마트카드를 이용한 원격 사용자 인증 스킴을 제안하였다. 이 스킴은 시스템 유지에 패스워드 테이블(password table)를 사용하지 않도록 했다는 점에서 새로운 모델을 제시하였다. 최근에 Sun [5]은 Hwang과 Li가 제안한 스킴과 같은 이점을 주면서, 통신 및 계산비용(communication and computation cost)를 상당히 줄이는 모델을 제시하였다. 본 논문은 앞에서 제시된 모델들의 약점과 보완점을 해결하고자 이산대수와 해쉬 함수를 결합한 하이브리드 방식으로 양방향 인증을 제공하는 모델을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 Hwang과 Li의 방식과 Sun의 방식에 대해 정리하고, 3장에서는 제안한 스킴에 대한 설명, 4장에서는 제안한 스킴에 대한 안전성 분석, 5장에서는 다른 스킴들과 비교하여 성능을 분석하고, 최종적으로 6장에서 결론을 맺는다.

2. 관련 연구

2.1 Hwang과 Li의 방식

Hwang과 Li의 스킴 [2]의 안전성은 이산 대수 문제의 풀기 어려움을 기반으로 등록 단계, 로그인 단계 그리고 인증 단계로 구성이 되어 있다.

등록 단계:
새로운 사용자(user)가 자신의 아이디 ID_i를 등록을 위해 시스템에 제출한다고 가정하자. 시스템은 사용자에게 대한 패스워드 PW_i를 다음과 같이 계산한다

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

여기에서 x_s는 시스템에서 갖고 있는 비밀키이다. 등록 센터는 공개쌍 파라메터(h, P)을 포함한 스마트카드를 발행한다. 여기에서 h는 일방향 함수이다. 등록 센터는 또한 보안 채널을 통해 사용자에게 PW_i를 배달한다.

로그인 단계:
만일 사용자가 로그인하기를 원한다면, 스마트카드를 입력장치에 넣으면 된다. 그 후 사용자는 자신의 아이디 ID_i와 패스워드 PW_i를 입력장치에 입력한다. 스마트카드는 다음과 같은 기능을 수행한다.

1. 랜덤 넘버(random number) r을 생성한다.
2. $C_1 = ID_i^r \bmod P$ 를 계산한다.
3. $t = f(T \oplus PW_i) \bmod (P-1)$ 을 계산한다. 여기에서 T는 현재의 날짜와 시간이며 $\oplus$는 exclusive operation을 나타낸다.
4. $M = ID_i^t \bmod P$를 계산한다.
5. $C_2 = M(PW_i)^r \bmod P$를 계산한다.
6. 메시지 C = (ID_i, C_1, C_2, T)를 시스템에 보낸다.

인증 단계:
인증을 요구하는 메시지 C를 받으면, 시스템은 다음과 같은 단계를 사용하여 로그인 사용자를 인증한다. 시스템은 메시지를 T'에 받는다고 가정하고, 여기에서 T'는 시스템의 현재 날짜와 시간이다.

1. ID_i의 유효성(validity)을 확인한다. 만약 ID_i의 형식이 정확하지 않으면, 시스템은 요구(request)를 거절한다.
2. replaying attacks을 견디기 위하여 T와 T'사이의 시간 간격의 유효성을 확인한다. 만약 $(T'-T) \geq \Delta T$ 이면, 여기에서 ΔT는 전송 지연에 대한 유효한 시간 간격을 가르키고, 시스템은 request를 거절한다.
3. 시스템은 $PW_i = ID_i^{x_s} \bmod P$와 $t = h(T \oplus PW_i) \bmod (P-1)$ 을 계산한다. 만약 $C_2 (C_1^{x_s})^{-1} \bmod P = ID_i^t \bmod P$ 이면, 시스템은 request를 승인하고 그렇지 않으면 request를 거절한다.

2.2 Sun의 방식

Sun 스킴 [5]은 one-way function을 기반으로 한다. 이 스킴은 다음과 같은 3단계로 구성되어있다.

등록 단계:
x는 시스템이 갖고 있는 비밀키이다. h는 one-way function이다. 새로운 사용자(user)는 등록을 위해 시스템에 자신의 아이디 ID_i을 제출한다. 시스템은 사용자에 대한 다음과 같은 과정을 통해 패스워드 PW_i를 계산한다.

$$PWi = h(IDi, x)$$

등록 센터는 공개 일방향 함수 h을 포함한 스마트카드를 발행한다. 등록 센터는 또한 비밀 채널을 통해 사용자에게 PW_i를 배달한다.

로그인 단계:
만일 사용자가 로그인하기를 원한다면, 입력 장치에 자신의 스마트카드를 입력한다. 그 후 자신의 아이디 ID_i와 패스워드 PW_i을 입력 장치에 입력한다. 스마트카드는 다음의 과정을 수행한다.

1. $C_1 = h(T \oplus PW_i)$ 를 계산한다. 여기에서 T는 현재 날짜와 시간이다.
2. 메시지 $C = (ID_i, C_1, T)$ 를 시스템에 보낸다.

인증 단계:
인증을 요구하는 메시지 C가 도착한 후에, 시스템은 다음과 같은 단계를 사용하여 로그인 사용자를 인증한다. 시스템은 메시지 C를 T'에 받는다. 여기서 T'는 시스템의 현재 날짜와 시간이다.

1. ID_i의 유효성을 확인한다. 만약 ID_i의 형식이 정확하지 않다면, 시스템은 request를 거절한다.
2. replaying attack을 대비하여 T와 T'사이의 시간 간격의 유효성을 체크한다. 만약 $(T' - T) \geq \Delta T$ 이면, 여기에서 ΔT 는 전송 지연에 대한 유효한 시간 간격을 가르키고, 시스템은 request를 거절한다.
3. 시스템은 $PW_i = h(ID_i, x)$ 와 $C_1' = h(T \oplus PW_i)$ 를 계산하고, C_1'와 C가 같으면 request를 승인하고, 그렇지 않으면 request를 거절한다.

3. 제안하는 인증 스킴

이 장에서는 스마트카드를 사용한 원격 인증에 대한 효율적인 스킴을 제안하겠다. 제안된 스킴은 이산대수와 해쉬 함수를 혼합한 하이브리드 방식을 사용하였다. 제안된 스킴은 다음과 같이 3단계의 흐름으로 구성되어 있다.

등록 단계:
시스템의 비밀키를 d라하고, 새로운 사용자가 자신의 아이디 ID_i를 등록을 위해 시스템에 제출한다고 가정하자. 시스템은 다음과 같이 패스워드 PW_i를 계산한다.

$$PW_i = (ID_i)^d \bmod P$$

시스템은 안정된 보안 채널을 통해 사용자의 PW_i를 배달한다.

로그인 단계:
만약 사용자가 로그인하기를 원한다면, 자신의 스마트카드를 입력 장치에 삽입한다. 그리고 자신의 아이디 ID_i와 패스워드 PW_i를 입력한다. 스마트카드는 다음과 같은 작용을 수행한다.

1. $C_1 = h(ID_i \oplus T \oplus PW_i)$ 를 계산한다. 여기에서 T는 현재날짜와 시간이다.
2. 메시지 $C = (ID_i, C_1, T)$ 를 시스템에 보낸다.

인증 단계:
인증을 요구하는 메시지 C를 받고나면, 시스템은 다음과 같은 단계를 사용하여 로그인 사용자 인증을 한다.

1. 시스템은 ID_i의 유효성을 확인한다. 만약 ID_i의 형식이 정확하지 않다면, 시스템은 요구(request)를 거절한다.
2. replaying attacks으로부터 보호하기위해 T와 T'의 시간 간격 $(T' - T < \Delta T)$을 확인한다. 여기에서 T'는 요구 메시지가 도착했을 때의 타임 스탬프(timestamp)이다.
3. 시스템은 $PW_i = (ID_i)^d \bmod P$과 $C_1' = (ID_i \oplus T \oplus PW_i)$를 계산한다. 그리고 $C_1' ?= C_1$ 인지를 확인하고, 만약 비교값이 같지 않으면 요구를 거절한다. 반면에 시스템이 사용자의 요구를 수용하면 다음 4로 넘어간다.
4. 시스템은 현재의 타임 스탬프 T"를 해쉬 함수의 매개 변수에 삽입하고, $C_2 = h(T'' \oplus PW_i)$ 를 스마트카드로 돌려 보낸다.
5. 스마트카드는 메시지 $C_2' = h(T'' \oplus PW_i)$ 를 계산하고, $C_2' ?= C_2$ 인지를 확인한다. 인증이 확인이 되면 이것으로 양방향 인증이 실행된 것이다. 그렇지 않다면 연결은 차단된다.

4. 안전성(security) 분석

이 장에서는 제안한 스킴의 안전성을 분석한다.

1. replaying attacks의 경우 인증 단계 2에서 보듯 메시지의 유효성을 timestamp를 통해 확인하므로 메시지는 보호받는다.
2. 침입자(attacker)가 과거의 값을 수정하여 인증 단계 2를 통과하더라도, 이와 같은 수정은 $C_2 \neq h(T'' \oplus PW_i)$때문에 인증 단계 3을 통과할 수 없다.
3. C_1이 PW_i에 의해 유도되기 때문에, 유효한 PW_i를 모르는 사람은 $C = (ID_i, C_1, T)$ 값을 위조하여 생성할 수 없다.
4. 법적인 사용자가 인증을 통해 다른 합법적인 사용자의 아이디와 패스워드를 계산하려 하여도, 사용자의 아이디는 해쉬 함수로 전달되므로 해쉬 함수의 one-way특성에 의해 다른 사용자의 아이디와 패스워드는 보호받는다.
5. P값과 d값을 시스템이 갖고 있으므로, 합법적인 사용자가 다른 합법적인 사용자의 아이디와 패스워드를 구할 수 있는 공격을 원천적으로 봉쇄한다.

5. 성능 분석

이 장에서는 제안한 스킴의 몇 가지 성능 이슈를 앞에서 소개한 Hwang과 Li의 스킴과 Sun 스킴과 비교하여 분석한다.

표 1 스마트카드기반 스킴 사이의 메시지 길이 비교

	Key Length	Message Length
Hwang-Li's scheme	1024	2048
Proposed scheme	128	128

여기에서 Hwang과 Li가 제안한 스킴의 P는 이산대수 문제의 어려움을 위해 1024bits로, Sun과 새로 제안한 스킴의 해수 함수 h는 128bits로 가정한다. 표 1은 새로 제안한 스킴과 다른 스킴간의 키 길이와 메시지 길이를 비교한 것이다. 표 2는 새

로 제안한 스킴과 다른 스킴간을 비교한 것이다. 본 논문에서 제안한 스킴은 스마트카드분야에서 공개과라매터로 해쉬함수 h 만을 필요로 하므로 Hwang과 Li의 스킴이 필요로 하는 공개파라매터 (h, P)에 비해 매모리를 절약하는 이점을 갖고 있다. 이 점은 스마트카드에서 공개정보로 h값만을 갖게 함으로써, 매우 적은 양의 데이터를 전송하는 스마트카드의 효율성을 고려한 것이다. Hwang과 Li의 스킴에 있어서 합법적인 사용자의 아이디와 패스워드를 안다고 가정할 경우, 다른 사용자의 아이디와 패스워드를 알수 있는 약점이 밝혀졌다 [8]. 이러한 문제점을 극복하기 위해 P값을 서버의 비밀키로 유지함으로써 ID와 PW의 재사용 공격에 대한 대책으로 마련하였다.

표 2 스마트카드기반 스킴 사이의 비교

	Hwang-Li scheme	Sun scheme	제안 scheme
Verification table	no	no	no
Mutual authentication	no	no	yes
Computation of registeration phase	1 Exponential	1 hashing	1 Exponential
Computation of login phase	3 Exponential + 1 hashing	1 hashing	1 hashing
Computation of authentication phase	3 Exponential + 1 hashing	2 hashing	1 Exponential + 3 hashing
Public information stored in smart card	(h, P)	h	h

표 3은 window 2000 SP Celeron 850MHz에서 Ctypto++을 실험한 결과로 관련 스킴의 암호화 과정 시간을 나타낸 것이다.

표 3. 관련 스킴의 암호화 과정 시간

Algorithm		Operation time (millisecond)
ElGamal	1024 Encryption	11.03
	1024 Decryption	5.77
MD5		$62*10^{-3}$

본 논문에서 제안한 스킴은 스마트카드와 시스템사이의 메시지 전달시 hashing operations으로 매우 적은 양의 전송 데이터를 갖는 장점을 갖고 있다.

6. 결론

정보의 보안을 가장 효율적으로 보장하는 방법은 암호 시스템을 구축하는 것이다. 정보 보호를 위한 암호화 시스템 구축은 암호화 기법을 응용한 것으로 이러한 암호화 기법은 여러 분야에서 연구가 진행 중이다. 본 논문에서는 패스워드 파일이나 확인 테이블 사용을 완전히 버린 새로운 스마트카드를 이용한 양방향 인증 스킴을 제안하였다. 본 논문에서 제안한 스킴이 갖는 장점은 (1)확인 테이블이 필요하지 않고; (2)스마트카드와 시스템 사이에 양방향 인증을 제공하고; (3)Hwang-Li's 스킴의 약점을 극복했고; (4)이산대수와 해쉬함수를 혼합한 새로운 스킴을 제안했다는 것이다. 스마트카드 기반 스킴은 원격 인증에 있어 전도 유망하고 실질적인 실효성있는 솔루션이다. 본 논문에서 제안하는 스킴의 응용분야로는 스마트카드를 이용한 전자지불 시스템, 전자 화폐, 모바일 결제 카드등을 위한 연구가 계속적으로 진행되어야 할 것이다.

참고문헌

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

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

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

[4] M. S. Hwang, "A remote password authentication scheme based on the difital signature method," International Journal of Computer Mathematics, Vol. 70, 1999, pp. 657-666.

[5] Sun, "An Efficient Remote Use Authentication Scheme Using Smart Cards," IEEE Transaction on Consumer Elertroncis, Vol. 31, 1985, pp. 469-472.

[6] T. ElGamal, "A Public-key cryptosystem and a signature scheme based on discrete alogarithms," IEEE Trans, on Information Theory, Vol. 31, 1985, pp. 469-472.

[7] Mike Heendry, "Smart card security and application Second Edition," Trtech House, 2001.

[8] Chan and Cheng, "Cryptanalysis of a Remote User Authentication Scheme Using Smart Cards," IEEE Transactio non Consumer Electronics, Vol. 46, No. 4, November, 2000