스마트카드에 적합한 효율적인 영지식 개인식별 방식

김태훈, 이보영, 원동호
성균관대학교 정보공학과

Efficient Zero-Knowlege Identification Scheme fitted for Smart Cards

Tae-Hoon Kim, Bo-Young Lee, Dong-Ho Won

Department of Information Engineering
Sung Kyun Kwan University
thkim@dosan.skku.ac.kr
http://dosan.skku.ac.kr/~thkim

요약

일반적으로 스마트 카드에서의 사용자 인증은 사용자가 제출하는 패스워드나 PIN을 스마트 카드내의 것과 비교하여서 이루어지고 있으며, 카드/리더기 인증은 암호프로토콜을 사용함으로써 이루어지고 있다. 본 논문에서 제시하고자하는 새로운 프로토콜은 [9]에서 제안된 모델을 바탕으로 구현한 것으로 사용자 인증과 스마트 카드 인증을 동시에 수행할 수 있으며 키관리측면에 있어서 효율적이며 오프라인이 가능하다.

1. 서론

스마트카드를 사용하여 인증을 수행할 때 크게 사용자 인증과 개체 인증으로 나누어 볼 수 있다. 사용자 인증은 카드의 운영체제(COS)에 의한 접근제어(access control)로 이루어 진다. 사용자에 의해 제출된 PIN은 스마트카드로 전송되어지며 스마트카드의 운영체제는 이를 자신의 비밀영역(secret zone)에 있는 PIN과 비교하여 사용자 인증을 완료하게 된다. 사용자 인증은 카드제조시 미리 정해진 회수만큼의 제한을 두어 잘못된 PIN이 정해진 회수를 넘게 제출되었을 경우 카드는 기능을 잃게 된다. 개체 인증(entity authentication)은 카드와 터미널 CAD(Card Adapter Device)-카드리더기-사이, 그리고 터미널과 중앙의 호스트 컴퓨터사이의 인증을 일컫는다. 카드와 터미널 사이에서 이루어지는 개체인증을 통하여 카드나 터미널은 서로 정당한 개체인지를 암호학적으로 검증하게 된다.

본 논문에서는 [9]에서 제안된 사용자인증과 개체인증을 동시에 수행하는 모델을 기존의 영지식 개인식별 방식(zero-knowledge identification scheme)에 적용한 프로토콜을 제시한다. 제 2장에서는 스마트카드를 이용한 기존의 인증방식들에 대하여 알아보고, 제 3장에서는 영지식증명방식을 이용한 개인식별 방식에 관하여 알아보고, 관용키, 공개키 방식등과 비교, 고찰해 보았다. 제 4장에서는 [9]의 모델을 바탕으로 사용자인증이 가능한 영지식 개인식별 방식을 제안하였다.

2. 기존의 스마트카드 인증

기존의 스마트카드를 사용하여 인증을 할 때는 사용체인증과 개체인증을 별도로 수행하였다. 이를 도식화해보면 그림 1.과 같다.[1]

사용자인증(user authentication)은 사용자가 입력한 PIN을 가지고 수행하는 접근제어(access control)이며, 개체 인증은 검증자(verifier)가 질문을 보내면 증명자(prover)가 여기에 답을하는 challenge-response 프로토콜로서, 주로 스마트카드가 증명자가 되며 터미널은 검증자가 되는데 상호인증을 수행할 수도 있다. 개체 인증시에 사용되는 방식으로는 크게 관용키방식, 공개키방식, 그리고 영지식증명방식을 들 수 있는데, 이들은 결국 증명자가 정당한 비밀키를 가지고 있다는 것을 검증자에게 증명하는 것이다.

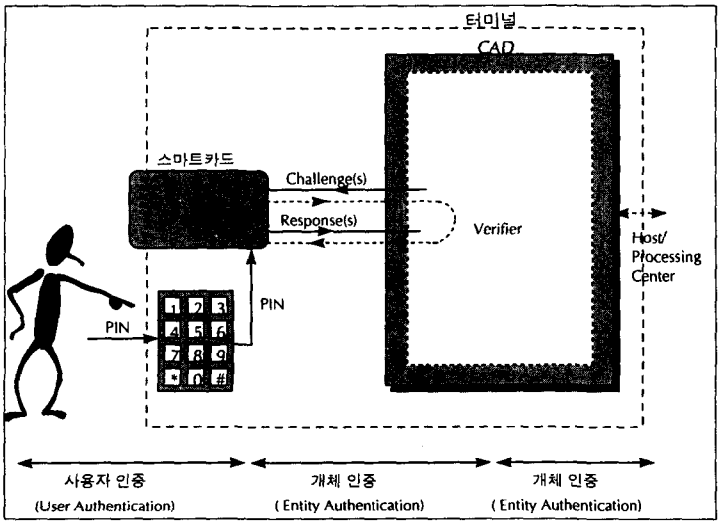

그림 1. 스마트카드를 사용한 기존의 인증 모델[1]

관용키 인증 방식은 검증자측과 증명자측이 같은 키를 가지고 인증을 수행하는 것이며, 공캐키 인증 방식은 스마트카드의 비밀키와 이에 해당하는 공개키를 사용하여 인증을 수행하는 것인데 (비밀키, 공개키)쌍은 서로 수학적으로 밀접한 관련이 있으나 공개키로부터 비밀키를 알아내는 것은 아주 어려워야 한다. 공개키 인증방식에서 스마트카드는 자신의 공개키를 터미널로 전송하게 되는데, 이때 터미널은 공개키방식의 특성상 공개키인증을 해야한다.

3. 영지식 개인식별

이 방법은 신분(identity)의 증명을 zero-knowledge 증명방식을 사용해서 수행하는 것인데 Feige, Fiat, Shamir에 의해 처음으로 제안[6]되었다.

영지식 증명방식은, 각 라운드 계산량은 공개키 방식에 비해 적으며, 안전도는 프로토콜의 반복회수(challenge, response쌍)에 지수적으로 비례한다. 신분의 증명을 원하는 사람은 자신의 비밀키를 노출시키지 않고 자신이 비밀키를 가지고 있음을 증명함으로써 그의 신분(identity)을 증명하는 것이다. 계산량, 메모리 사용량 등이 보통의 공개키 방식보다 유리하므로 스마트 카드 응용에 보다 적합한 모델이 될 수 있다.[3] 그림 2.는 영지식 개인식별 방식의 일반적 모델을 도식화해 본 것이다.[2]

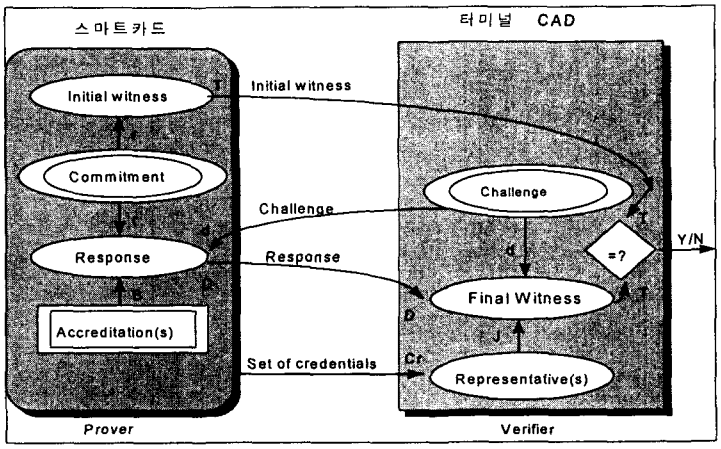

그림 2. 일반적인 영지식 개인식별[2]

표 1.은 각 프로토콜의 특징을 일반적으로 나타내어 본 것이다. 표에서 볼 수 있듯이 영지식 증명방식을 이용하는 것이 스마트카드에 유리하다. 물론 계산량, 메모리 사용량 등에서 관용키방식이 유리하나 키관리에 문제가 발생하기 때문에 적합하지 않으며, 키관리 문제를 해결하기 위해 터미널에서 사용하는 마스터키나 난수초기값(random seed)이 공격당한 경우는 전체시스템에 영향을 미치게 된다.

Protocol의 종류 (Family)	메시지크기 (Message Size)	연산횟수 (Protocol Iteration)	계산량 (Amount of Calculation)	메모리사용량 (Memory Requirement)
Zero-knowledge	large	many	large	large
공개키(Public-key)	large	one	very large	large
관용키(Symmetric)	small	one	small	small

표 1. 각 방식의 비교[11]

trap-door 공개키방식은 관용키방식에 비해서 많은 장점을 지니나 512bit이상의 큰 수를 다루기 때문에 스마트카드에는 큰 부담이 된다. 그러나 영지식 개인식별방식은 스마트카드에 적용하기에 적합한 특성을 지닌다. 다음 표는 여러 측면에서 공개키방식들을 비교해 본 것이다.[10]

n은 모듈러, k는 비밀키의 수, t는 FS[6]의 반복회수, s와 e는 RSA[5]비밀키와 공개키, v는 GQ[8]의 비밀파라메타이다.

Algorithm	Security level	No. modular mult.	No. bits exchanged	No. 512bit RAM	No.secret bits	No.public bits
RSA		3/2|n|	2|n|	2-3	|s|	|n|+|e|
FS	2^{-kt}	(k/2+1)t	(2|n|+k)t	1-2	k|n|	|n|
GQ	v^{-1}	3|v|+1	2|n|+|v|	2-3	|n|	|n|+|v|

표 2. 몇 공개키 알고리즘의 비교[10]

4. 사용자 인증이 가능한 영지식 개인식별 프로토콜

기존의 스마트 카드 인증은 사용자인증, 개체인증을 각기 수행하였다. 즉 자신만이 알고있는 것에 기반을 둔 사용자 인증과 자신만이 소유하고 있는 것에 기반을 둔 카드 인증을 따로 하고 있는 것이 특징이다. 저자들은 [9]에서 계산능력에 한계가 있는 카드를 사용하여 사용자인증과 개체인증을 동시에 수행하는 모델을 제시하였다. 본 논문에서는 이러한 모델을 만족하는 효율적인 영지식 인증방식을 제안한다. 즉 사용자 인증과 카드 인증을 따로 하지 않고 동시에 수행하면서 두 가지 기능을 동시에 수행하는 방법이다. PIN이나 인증시 사용되는 키 어느 것이라도 부정한 것이라면 인증프로토콜을 통과할 수 없다. 다음은 영지식 증명방식을 이용하여 프로토콜을 구현해 본 것이다.

Fiat-Shamir[7] 개인식별 방식을 이용해서 사용자인증과 개체인증을 동시에 수행하는 프로토콜을 살펴보자.

* 시스템설정

① 센터는 두 개의 큰 소수 p, q 선택하여 n을 계산한다.

$$n = p * q$$

② 식별자 I를 정한 다음 mod n상에서 평방잉여가 되는 v_i를 계산해 낸다. 공개키는 I와 집합 j가 된다.

$$v_j = H(I, j) \ , \ j = 1,\sim,k$$

③ 비밀키는 다음 식을 만족하는 가장 작은 s_i를 계산한다. 그리고 PIN을 선택한다.

$$s_j = \sqrt{v_j^{-1}} \ (\mathrm{mod}\ n)$$

④ 센터는 자신만이 아는 trap-door정보로 다음 식을 만족하는 집합 x를 계산한 후, 스마트카드에 넣어 발급한다. 단 $f_{td}()$는 trap-door 일방향함수, trap-door정보는 센터가 비밀리에 보관한다.

$$f_{td}(x, PIN) = s_j \ , \ j = 1,\sim,k$$

* 인증절차

① 사용자가 키패드를 통해 PIN을 입력한다. 이는 스마트카드로 전송된다.
② 스마트카드가 식별자 I를 터미널에 전송하면, 터미널은 H(I, j)로 v_j, (j = 1,~,k)를 계산한다.
③ 스마트카드는 비밀영역의 x와 입력된 PIN을 다음 식의 입력 값으로하여 s_j를 비밀키로 사용한다.

$$s_j = f_{td}(x, PIN)$$

④ 스마트카드는 난수 r을 발생시킨 후 다음 식을 계산하여 터미널로 전송한다.

$$w = r^2 \pmod n$$

⑤ 터미널은 랜덤한 이진벡터(b_1, ~,b_k)를 발생시켜 스마트카드로 전송한다.(challenge)
⑥ 스마트카드는 다음 식을 계산하여 전송한다.(response)

$$y = r \prod_{b_j=1} s_j \pmod n$$

⑦ 터미널은 다음 식으로 검증한다.

$$w = y^2 \prod_{b_j=1} v_j \pmod n$$

4번 이하의 과정을 t회 반복한다.

또한, Guillou-Quisquater[8] 개인식별 방식을 이용한 사용자인증과 개체인증을 동시에 수행하는 프로토콜을 살펴보면 다음과 같다.

* 시스템설정

① 센터는 두 개의 큰 소수 p, q 선택하여 n을 계산한다.

$$n = p * q$$

② 센터는 J = Red(I)를 구한 후, 다음 식을 계산한다. (단, Red()는 redundancy rule이다.)

$$A = J^{1/v} \pmod n \text{ 계산}$$

③ 비밀키로 A의 역원 B를 계산하고, PIN을 선택한 후, 자신만이 아는 trap-door정보로 다음 식을 만족하는 x를 계산하여 스마트카드에 저장한다. 단 f_{td}()는 trap-door 일방향함수, trap-door 정보는 센터가 비밀리에 보관한다.

$$JB^v = 1 \pmod n,$$

$$B = f_{td}(x, PIN)$$

* 인증절차

① 사용자가 키패드를 통해 PIN을 입력한다. 이는 스마트카드로 전송된다.
② 스마트카드가 식별자 I를 터미널에 전송하면, 터미널은 다음을 계산한다.

$$J = Red(I)$$

③ 스마트카드는 비밀영역의 x와 입력된 PIN을 다음 식의 입력 값으로하여 비밀키 B로 사용한다.

$$B = f_{td}(x, PIN)$$

④ 스마트카드는 난수 r을 발생시켜 다음 식을 계산하여 터미널로 전송한다.

$$T = r^v \pmod n$$

⑤ 터미널은 난수 $d \in [0, v-1]$를 발생시켜 스마트카드로 전송한다.(challenge)
⑥ 스마트카드는 다음 식를 계산하여 전송한다.(response)

$$D = rB^d \pmod n$$

⑦ 터미널은 다음 식을 만족하는지 검증한다.

$$T = D^v J^d \pmod n$$

5. 결론

본 논문에서는 사용자코드(PIN)로부터 만들어진 비밀키를 가지고 사용자인증과 카드 인증을 동시에 수행하는 모델을 기존의 영지식 개인식별 방식에 적용하였다. 본 방식에서는 제출된 PIN과 비밀정보가 결합된 비밀키를 가지고 인증을 수행하기 때문에 PIN이나 비밀정보가 하나라도 부정한 것일 경우에는 인증을 통과할 수 없다.

본 방식은 속도, 터미널과 카드사이의 통신량, 중간 계산값을 위한 RAM의 용량, 비휘발성메모리(NVM)의 용량 등을 비교해 볼 때 trap-door를 사용한 일반적 공개키방식(예, RSA[5])보다 스마트카드 적용에 유리하다.

참고문헌

[1] Hans-Peter Königs, "Cryptographic Identification Methods for Smart Cards in the Process of Standardization", IEEE Communications Magazine, pp.42~48 , June 1991
[2] Simmons, G.J. (Ed.) , "Contemporary Cryptology : The science of information integrity", IEEE PRESS, chap.12, 1992
[3] Bruce Schneier , "Applied Cryptography", John Wiley & Sons, Inc, 1994
[4] J. L. Zoreda, J. M. Oton , "Smart Cards", ARTECH HOUSE, INC chap.3, chap.5, 1994
[5] Revest, Shamir, Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", Comm. ACM, vol.21, no.2, pp.120-126, 1978
[6] Fiat, Shamir, "How to Prove Yourself : Practical Solution to Identification and Signature Problem", CRYPTO'85 Lecture Notes in Computer Science, vol.263, pp.186-194, Springer-Verlag, 1986
[7] Feige, Fiat, Shamir, "Zero-Knowledge Proofs of Identity", Journal of Cryptology 1988,

pp.77-94

[8] Guillou, Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors and Minimizing Both Transmission and Memory", EUROCRYPT'88. Lecture Notes in Computer Science, Springer- Verlag

[9] 김 태 훈, 김 승 주, 원 동 호, "스마트 카드에 적합한 효율적인 인증 모델", 한국통신학회 하계종합학술발표회 논문집 상권, pp. 605-608, 1996.7

[10] J.-F. Dhem, D.Veithen and J.-J. Quisquater, "SCALPS:Smart Card Applied to Limited Payment Systems", UCL Crypto Group Technical Report Series, http://www.dice.ucl.ac.be/crypto/

[11] Hannu A.Aronsson,"Zero Knowledge Protocols and Small Systems", http://www.niksuls.cs.hut.fi/~haa/nonpub/zeroknowledge.html