키로밍 서비스를 제공하는 새로운 개인키 관리 프로토콜

이용호, 이임영
순천향대학교 정보기술공학부

New PKM protocol supporting Key Roaming service

Yong-do Lee, Im-yeong Lee
Division of Information Technology Eng. Soonchunhyang University

요 약

정보화 사회가 도래하면서 정보보호의 중요성이 강조되고 있으며, 정보보호 서비스를 제공하기 위한 기반 구조로써 공개키 기반 구조가 구축되어 사용되고 있다. 공개키 기반 구조는 공개키 암호 방식을 사용하는 암호시스템에서 사용자의 공개키를 안전하고 신뢰성 있게 관리하는 수단을 제공한다. 그러나 사용자들의 개인키에 대한 관리 기술은 미비한 실정이다. 최근들어 암호 프로토콜을 이용하여 개인키를 안전하게 관리하기 위한 개인키 관리(PKM; Public Key Management) 프로토콜이 연구되고 있다.

이에 본 논문에서는 공개키 암호 기술에서 사용되는 개인키를 안전하게 관리하고, 키 로밍 서비스를 제공할 수 있는 새로운 PKM 프로토콜을 제안하였다.

I. 서 론

공개된 네트워크인 인터넷의 확산은 우리들의 생활에 많은 변화를 가져왔다. 특히, 가상 공간에서 이루어지는 전자상거래는 사용자들에게 효율성과 편리성을 제공하고 있다. 그러나 인터넷이 가지고 있는 특징에 의해 개인이나 기업 더 나아가서는 국가차원의 중요한 정보가 노출될 수 있다는 위험성을 가지고 있다.

암호 기술은 인가되지 않은 사용자로부터 정보를 보호할 수 있는 방법으로써 다양하게 연구되고 있다. 현재 대부분의 선진국들은 공개키 기반 구조(PKI; Public Key Infrastructure)를 구축하여 인증, 무결성, 기밀성, 부인봉쇄 등과 같은 다양한 암호 서비스를 제공하고 있다. PKI상에서 사용자는 인증기관(CA; Certificate Authority)에 등록하여 자신의 개인키 및 공개키를 생성하고, 공개키 인증서를 발행 받는다. 이렇게 사용자의 공개키는 PKI에 의해 안전하게 관리된다.

그러나 사용자의 개인키를 관리하는 기반 구조에 대한 연구는 미비한 실정이다. 기존에는 개인키를 PC의 하드디스크나 스마트카드와 같은 저장매체에 저장하여 관리하고 있다. PC와 같은 경우는 사용자의 이동성을 제공하지 못하며, 스마트카드와 같은 경우는 사용자가 항상 소지해야 하고 카드 리더기와 같은 부가적인 장비가 필요하기 때문에 불편함이 생길 수 있다.[2]

이러한 문제점들을 해결하기 위한 방안으로 사용자의 개인키를 안전하게 관리하기 위한 개인키 관리(PKM; Private Key Management) 프로토콜에 대한 연구가 활발히 진행되고 있다. PKM 프로토콜은 사용자에게 키 로밍 서비스를 제공할 수 있다는 특징을 가지고 있다.[1]

본 논문에서는 공개키 암호 기술에서 사용되는 개인키를 안전하게 관리하고, 키 로밍 서비스를 제공할 수 있는 새로운 PKM 프로토콜을 제안한다. 논문의 구성은 다음과 같다. 2장에서는 PKM 제품에 대해 소개하고, 3장에서 제안 방식을 기술한다. 마지막으로 4장에서 결론을 맺도록 한다.

II. PKM 제품

1. Hush Enterprise 제품

1) 등록 단계

그림 1은 Hush Enterprise 제품의 등록 단계를 나타내고 있다.[1]

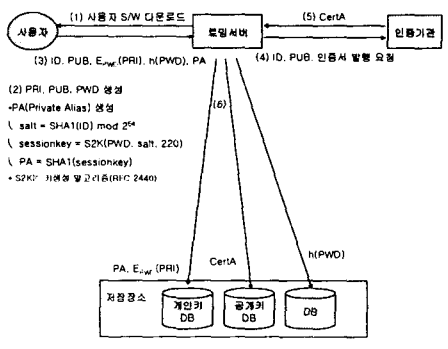

그림 1 : Hush Enterprise 제품의 등록 단계

2) 키로밍 단계

그림 2는 Hush Enterprise 제품의 키로밍 단계를 나타내고 있다.[1]

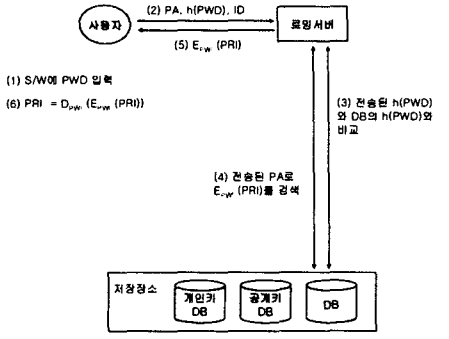

그림 2 : Hush Enterprise 제품의 키로밍 단계

3) 제품 분석

여기서는 Hush Enterprise 제품의 특징을 알아본다.[1]

· 개인키 DB로부터 개인키와 사용자간의 연결 정보를 직접적으로 알아낼 수 없다.

· 로밍서버의 사용자 위장 공격이 가능하다.

· 패스워드 기반의 취약점을 가지고 있다.

· 공개키 DB를 로밍서버가 운영한다. 그러나 전체 흐름에서 사용되지 않는다.

· 사용자와 로밍서버간에 SSL을 이용한다.

2. UniCERT Roaming 제품

1) 등록 단계

그림 3은 UniCERT Roaming 제품의 등록 단계를 나타내고 있다.[1]

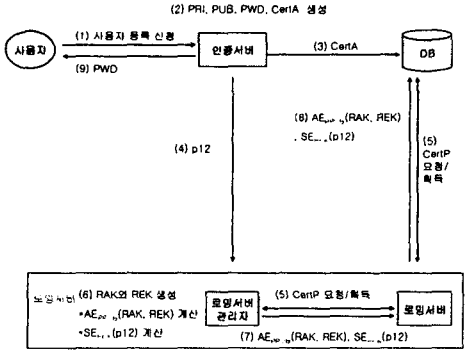

그림 3 : UniCERT Roaming 제품의 등록 단계

2) 키로밍 단계

그림 4는 UniCERT Roaming 제품의 키로밍 단계를 나타내고 있다.[1]

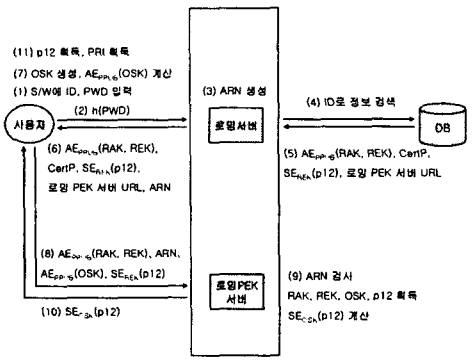

그림 4 : UniCERT Roaming 제품의 키로밍 단계

3) 제품 분석

여기서는 UniCERT Roaming 제품의 특징을 알아본다.[1]

· 인증서버는 사용자의 패스워드를 알고있다.

· 패스워드 인증자를 이용한 로밍서버의 사용자 위장 공격이 가능하다.

· 패스워드 기반의 취약점을 가지고 있다.

· 사용자와 로밍서버간의 안전한 채널 형성에 관한 내용을 언급하고 있지 않다.

· RAK가 로밍 요청시 사용되는 인증키라고 했는데 사용 방법에 대해 언급하고 있지 않다.

III. 제안 방식

본 장에서는 제안하는 PKM 프로토콜에 대해 설명하고 특징을 알아본다.

1. 제안 방식 개요

다음은 제안 방식에 참여하는 개체의 역할과 시스템 계수에 대해 설명한다.

1) 참여 개체의 역할

제안 방식은 사용자와 로밍서버로 구성되고, 각각 다음과 같은 역할을 수행한다.

· 사용자 A : 사용자는 패스워드를 이용하여 인증 정보와 개인키 정보를 생성하고, 이들을 로밍서버에 위탁한다. 이후에 사용자는 키 로밍 서비스를 제공받을 수 있게 된다.

· 로밍서버 RS_i : 사용자 개인키 정보의 일부분과 인증 정보를 저장하고 있는 서버로써 사용자의 요청시 키 로밍 서비스를 제공한다. 로밍서버는 키 정보의 분산 저장을 위하여 n개를 운영한다.

2) 시스템 계수

다음은 제안 방식에서 사용하는 시스템 계수에 대한 설명이다.

· * : 참여개체를 가리키는 지시자(A: a, RS_i: rs_i)

· p : 임의의 큰 소수

· g : GF(p)상의 원시원소

· ID_* : *의 식별자

· pwd : A의 패스워드

· CertA : A의 인증서

· x_*, y_* : *의 개인키, *의 공개키

· Sig() : 서명 알고리즘으로 생성한 서명문

· E() : 대칭키 알고리즘으로 생성한 암호문

· h : 안전한 일방향 해쉬함수

2. 프로토콜

제안 방식은 사전 단계, 등록 및 검증 단계, 키 로밍 단계로 나누어진다. 다음은 각 단계에 대해 설명이다.

1) 사전 단계

RS_i간에 수행되는 단계로써 사용자 등록 전에 수행되어야 하는 과정이다.

① 모든 RS는 비밀값 r을 안전하게 공유한다.

② RS_i는 R과 k_i 그리고 sigV를 계산하고, sigV를 공개한다.

$$R = g^r \bmod p$$

$$k_i = R^{x\_rsi} \bmod p$$

$$sigV = Sig_{x\_rsi}(R \| k_i \| ID_{RSi})$$

2) 등록 및 검증 단계

A와 RS간에 수행되는 단계로써 A는 RS에 등록하고, RS는 이를 검증하는 과정이 수행된다.

① A는 pwd를 이용하여 hp, hpv, EPK를 다음과 같이 계산한다.

$$hp = h(g^{pwd} \bmod p)$$

$$hpv = g^{hp} \bmod p$$

$$EPK = E_{hp}(x\_a \| CertA)$$

② A는 (t, n) threshold VSS 기술[3]을 이용하여 EPK의 부분 정보 $EPKB_i$를 생성한다.

$$EPKB_1, EPKB_2, \ldots, EPKB_n$$

③ A는 RS에서 공개한 sigV와 랜덤수 t 그리고 $EPKB_i$를 이용하여 T, RT, e_i, s_i, c_i를 다음과 같이 계산한다. 그리고 ID_A, T, s_i, c_i를 RS_i에 전송한다.

$$T = g^t \bmod p$$

$$RT = R^t \bmod p$$

$$e_i = h(k_i \| T \| EPKB_i)$$

$$s_i = t - x\_a * e_i \bmod p$$

$$c_i = E_{RT}(EPKB_i \| hpv)$$

④ RS_i는 전송된 정보와 r을 이용하여 RT를 계산하고, RT를 이용하여 c_i를 복호화한다. ID_A와 hpv 그리고 $EPKB_i$를 안전하게 저장한다.

$$RT = T^r \bmod p$$

⑤ RS_i는 다음을 검증하고 이상이 없으면 사용자에게 등록 완료 메시지를 전송한다.

$$e_i = h(k_i \| T \| EPKB_i)$$

$$RT = (y\_a^{e_i} * g^{s_i})^r \bmod p$$

검증 과정은 다음과 같다.

$$RT = (y\_a^{e_i} * g^{s_i})^r \bmod p$$

$$= (g^{x\_a*e_i - t - x\_a*e_i})^r \bmod p$$

$$= g^{r*t} \bmod p$$

3) 키 로밍 단계

A와 RS간에 이루어지는 단계로서 A는 RS에게 키 로밍 서비스를 요청하고, RS는 사용자에게 키 로밍 서비스를 제공하는 과정이 수행된다.

① A는 접근이 용이한 RS_i에 접속해서 다운로드 전용 S/W를 다운받아 설치한 후 pwd를 입력한다.

② S/W는 입력된 pwd를 이용하여 hp와 hpv를 계산한다.

$$hp = h(g^{pwd} \bmod p)$$

$$hpv = g^{hp} \bmod p$$

③ S/W는 RS_i의 공개키로 PDH_i을 계산한다.

$$PDH_{i1} = y\_rs_i^{hp} \bmod p$$

④ S/W는 랜덤수 z, PDH_{i1}, hpv를 이용하여 다음 정보를 구성하고, RS_i에게 전송한다.

$$ID_A \| E_{PDHi1}(z) \| h(z \| hpv)$$

⑤ RS_i는 전송된 ID_A에 해당하는 hpv를 검색하고 자신의 개인키를 이용하여 PDH_{i1}를 계산한다.

$$PDH_{i1} = hpv^{x\_rsi} \bmod p$$

⑥ RS_i는 PDH_{i1}를 이용하여 $E_{PDHi1}(z)$를 복호하고, h(z ‖ hpv)을 계산하여 전송된 정보와 비교한다. 이상이 없다면 그대로 진행한다.

⑦ RS_i는 랜덤수 n을 선택해서 PDH_{i2}와 SK를 계산한다.

$$PDH_{i2} = PDH_{i1} \oplus hpv \oplus z$$

$$SK = h(PDH_{i1} \| PDH_{i2} \| n \| z)$$

⑧ RS_i는 다음 정보를 구성하여 A에게 전송한다.

$$IDrsi \| E_{PDHi2}(n) \| h(n \| r) \| E_{SK}(EPKB_i)$$

⑨ S/W는 PDH_{i2}를 계산해서 $E_{PDHi2}(n)$를 복호하고, $h(n \| r)$를 계산해서 전송된 값과 비교한다. 이상이 없다면 그대로 진행한다.

$$PDH_{i2} = PDH_{i1} \oplus hpv \oplus r$$

⑩ S/W는 PDH_{i1}, PDH_{i2}, n, z를 이용하여 SK를 계산한 후 $E_{SK}(EPKB_i)$를 복호한다.

$$SK = h(PDH_{i1} \| PDH_{i2} \| n \| z)$$

⑪ S/W는 복호된 $EPKB_i$를 이용하여 EPK를 계산한다.

⑫ S/W는 hp로 EPK를 복호하여 x_a와 CertA를 사용자에게 제공한다.

3. 비교 분석

표 1은 제품과 제안 방식을 비교한 것이다.[1]

표 1 : 비교 분석표

	Hush Enterprise	UniCERT Roaming	제안 방식
키로밍 권한 분산	X	X	O
사용자 위장공격 방어	X	X	O
패스워드 공격 방어	X	X	O

IV. 결론

공개키 암호 기술에서는 개인키와 공개키가 사용된다. 키의 관리는 암호 기술을 사용하는데 있어서 가장 중요한 문제라 할 수 있다. 공개키는 공개키 기반 구조하에서 인증기관에 의해 안전하게 관리되고 있는 반면, 개인키는 사용자의 PC나 스마트카드와 같은 저장장치를 이용하여 관리되고 있다. 그러나 PC나 스마트카드를 이용하는 것은 안전성이나 효율성 등에서 많은 문제점을 가지고 있다.

이에 본 논문에서는 공개키 암호 기술에서 사용되는 개인키를 안전하게 관리하고, 키 로밍 서비스를 제공할 수 있는 새로운 PKM 프로토콜을 제안하였다. 향후 좀 더 안전하고 효율적인 기술에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] 박해룡, 권현조, 김지연, 김승주, "국외 키로밍 제품 개발 현황 분석", 한국정보보호학회지 제12권 제 4호, pp.104-124, 2002.

[2] 이용호, 이임영, "개선된 패스워드 기반 키 로밍 프로토콜", 한국통신학회 하계종합학술발표회, pp.592, 2002.

[3] T. Pedersen, "A threshold cryptosystem without a trusted party", Advanced in Cryptology-Eurocrypt'91, Springer-Verlag, LNCS 547, pp.522-526, 1991.