

위임 인증서를 기반으로 한 다단계 대리서명 방식의 확장

이여진 김중태 정일용
조선대학교 컴퓨터공학부

Extended Multi-level Proxy Signature based on Proxy Certificate

Yejin Lee Joongtae Kim Ilyong Chung
Dept. of Computer Engineering, Chosun University
{smile96@naver.com, kjtsy@hanmail.net, iyc@chosun.ac.kr}

요약 - 대리 서명은 디지털 서명 기술의 응용으로서 Mambo에 의하여 최초로 제안이 되었고, Araki에 의하여 다단계 대리 서명으로 확장되었다. 본 논문에서는 위임 인증서와 서명 검증자의 서명 생성 여부를 원 서명자가 추후 확인하는 프로토콜을 이용하여 부인 봉쇄 및 원 서명자의 보호가 이루어지는 효율적이고 안정적인 다단계 대리 서명 방식을 제안한다.

1. 서 론

대리서명은 대리서명자가 원 서명자를 대신하여 원 서명자의 서명과 동일한 효력을 갖는 대리서명을 생성하고 이를 검증하는 암호학적 프로토콜이다. 대리서명의 이해를 위하여 다음과 같은 경우를 생각해 볼 수 있다. 만일 어떤 조직의 간부가 정보통신망에 접속할 수 없는 지역으로 출장을 가는 경우에 그는 출장 기간 동안 어떤 문서에 대한 결재나 메일 등에 대한 응답을 위하여 그의 권한을 다른 사람에게 부여하여야 한다. 권한을 위임받은 자-대리서명자-는 그에 적절한 직무를 수행하게 되는 것이고 이를 원활하게 수행하도록 하는 개념이 대리서명인 것이다.

대리서명(Proxy Signature) 방식은 Mambo[1]-[2]에 의해서 처음 제안된 이후

많은 발전 과정을 거쳐서 오늘날 다양한 대리서명 방식이 제안되었다. 위의 예를 이용하여 가정을 추가하여 보자. 대리서명자 또한 출장을 가는 상황이 발생하였다면 그도 서명 권한을 위임하여야 할 것이다. 이렇게 서명 권한을 위임받은 자의 서명 권한을 다시 위임하는 것을 다단계 대리서명 방식이라 한다.

원활한 대리서명을 위하여 인증서 사용을 고려할 수 있는데 실제 조직에서 운용되는 인증서는 권한을 위임하기 위하여 인증서와 비밀키를 대리서명자에게 위임하여야 한다. 그러나 이 방법은 인증서의 모든 권한을 위임하는 의미를 내포하고 있어 보안상의 많은 문제점을 가지고 있다. 가장 큰 문제점은 대리서명자의 인증서와 비밀키의 오남용을 막기가 힘들다는 것이다. 또한 대리서명

후 직원의 부인방지를 막을 수 없으며 대리 서명자가 제삼자에게 원 위임자의 동의 없이 인증서와 비밀키를 알려 줌으로써 대리 서명 능력을 갖게 할 수 있다. 또한 비밀키의 노출이 반복적으로 일어남으로써 안전성에 심각한 문제를 일으킬 수 있다[6].

본 논문에서는 Tuecke[7]가 제안한 위임 인증서 개념과 원 서명자가 추후 확인이 가능하도록 하는 프로토콜을 이용하여 위임 부인을 방지하고 원 서명자를 보호할 수 있는 다단계 대리서명 확장 방식을 제안한다.

2. 대리 서명에 관한 연구

Mambo는 대리 서명 기법을 원 서명자의 서명 권한을 위임하는 형태에 따라 완전 위임, 부분 위임, 보증 위임 방식으로 나누어 제안하였다. 완전 위임 방식은 원 서명자가 대리 서명자에게 자신의 비밀키를 주는 경우로 대리 서명자의 서명과 원 서명자의 서명이 구분이 되지 않는 방식이다. 부분 위임은 완전 위임 보다 안전한 방식으로 원 서명자가 대리 서명용 비밀키를 자신의 비밀키를 이용하여 생성하는 방식이다. 이 때 비밀키는 대리 서명용 비밀키로부터 계산이 불가능하여야 한다. 보증 위임 방식은 원 서명자가 대리 서명자에게 보증서를 발행함으로써 대리 서명을 구현하는 방식이다.

Araki는 Mambo의 대리 서명 방식을 확장하여 다단계 대리 서명 방식을 제안하였다. Mambo의 대리서명 방식을 이용한 다단계 대리서명 방식은 서명용 키를 생성할 때 자신의 비밀키와 공개키를 사용하여 다시 서명용 키를 생성한다.

본 논문에서 제안하는 프로토콜 표기법은 <표 1>과 같다.

표 1. 프로토콜 표기법

표기법	
p, q	$q p-1$ 을 만족하는 큰 소수
g	위수가 q 인 Z_p 상의 원소
U_0	0번째 서명자(원 서명자)
U_i	i번째 대리서명자
x_i	i번째 대리서명자의 비밀키
y_i	i번째 대리서명자의 공개키, $y_i \equiv g^{x_i} \pmod{p}$
pC_i	i의 위임 인증서(proxy certificate)
e_i	pC_i 와 K_i (공개정보)로 해쉬함수를 적용한 결과값
σ_i	i번째 대리서명자의 대리서명용 비밀키
λ_i	i의 서명키
h	안전한 일방향 해쉬함수
$SIG_{u_i}(m)$	U_i 가 생성하는 메시지 m에 대한 전자서명
$Ver(Sig_{u_i}(m))$	U_i 의 전자서명에 대한 검증

3. 위임 인증서

위임 인증서는 대리 서명자가 대리 서명을 위한 키 쌍을 생성하고 이를 위임자의 이름과 묶어 서명을 한 인증서이다[7]. 다단계 대리 서명 시 다단계의 위임이 이루어지면 대리 서명자의 신원 확인은 필수적인 보안 요소가 되며, 위임 인증서 내에 대리인의 권한의 한계를 규정하여 위임 인증서의 사용에 명백한 제한을 가하는 요소가 필요

하다.

이와 같은 위임 인증서는 대리 서명자에 대한 여러 가지 정보를 담은 문서에 위임자가 서명을 함으로써 발급된다. 대리 서명자의 정보를 담은 부분에 위임 인증서의 유효 기간이나 대리서명자의 자격 요건 등 위임자가 원하는 권한 위임에 대한 제한 조건을 담아서 대리 서명자의 서명 능력을 제한할 수 있다[6]. 실생활에서 권한의 위임은 자주 일어나고 있으며 이를 위해서 대리 서명도 앞으로 반드시 필요한 정보 보호 서비스 중 하나가 될 것이다.

4. 제안 방식

본 논문에서는 Tuecke가 제안한 위임 인증서에 원 서명자의 정보를 추가적으로 삽입하여 위임 인증서를 재구성함으로써 원 서명자가 추후 확인이 가능하도록 하는 프로토콜을 설계하여 위임 부인을 방지하고 원 서명자 및 대리 서명자를 동시에 보호할 수 있는 다단계 대리서명 방식을 제안한다.

4.1 대리 서명용 키 생성

원 서명자 U_0 는 아래와 같이 대리 서명용 키를 생성하여 대리 서명자 U_i 에게 전송한다.

- 1) U_0 는 난수 $k_0 \in Z_{p-1}$ 을 선택한 후

$$K_0 \equiv g^{k_0} \pmod{p}$$
 를 계산한다.

- 2) U_0 는 자신의 서명정보와 대리 서명자의 정보가 포함된 위임 인증서 pC_0 와 K_0 을 가지고 $e_0 \equiv h(pC_0, K_0) \pmod{q}$ 을 계산한다.

- 3) U_0 는 대리 서명용 키

$$\sigma_0 \equiv x_0 e_0 + k_0 \pmod{q}$$
 를 계산한다.

- 4) U_0 는 σ_0, e_0, pC_0 를 안전한 채널을 통해 U_i 에게 전송한다.

i 번째 대리 서명자 U_i ($i > 0$)가 다른 대리 서명자 U_{i+1} 에게 원 서명자 U_0 의 서명 생성 능력을 위임하고자 한다면 다음 단계를 수행한다.

- 1) U_i 는 난수 $k_i \in Z_{p-1}$ 을 선택한 후 $K_i \equiv g^{k_i} \pmod{p}$ 를 계산한다.
- 2) U_i 는 $e_i \equiv h(pC_0 \parallel pC_1 \parallel \dots \parallel pC_i, K_i) \pmod{q}$ 를 계산한다.

이 때 이전에 받은 $pC_0, pC_1, \dots, pC_{i-1}$ 의 내용과 pC_i 를 연결하여 해쉬함수를 적용한다.

- 3) U_i 는 대리 서명 생성 키 $\sigma_i \equiv \sigma_{i-1} + x_i e_i + k_i \pmod{q}$ 를 계산한다.
- 4) U_i 는 $\sigma_i, (e_0, e_1, \dots, e_i), (pC_0, pC_1, \dots, pC_i)$ 를 U_{i+1} 에게 전송한다.

4.2 대리 서명용 키 검증

대리 서명자 U_i 는 U_{i-1} 에게 받은 정보와 U_{i-1} 의 공개키 y_{i-1} 와 대리 서명용 공개키를 이용하여 다음과 같이 대리 서명용 키를 검증한다.

- 1) $e_{i-1}' \equiv h(pC_0 \parallel pC_1 \parallel \dots \parallel pC_{i-1}, K_{i-1})$ 를 계산한 후 e_{i-1}' 과 같은지 확인한다.

- 2) 위 식이 성립하면

$$g^{\sigma_{i-1}} \equiv y_0^{e_0} y_1^{e_1} \dots y_{i-1}^{e_{i-1}} K_0 K_1 \dots K_{i-1} \pmod{p}$$
 를 확인한다.

위 식이 검증되면, U_i 는 U_0 의 대리 서명용 키 σ_i, λ_i 를 생성할 수 있다. 여기에서 λ_i 는 서명키이고, σ_i 는 다른 대리인에게 보내

는 대리 서명용 키이다.

$$\lambda_i \equiv \sigma_{i-1} + e_{i-1}x_i \pmod{q}$$

4.3 서명 생성 및 검증

U_i 는 일반적인 서명 방식을 이용하여 $SIG_{U_i}(m, \lambda_i)$ 대리 서명을 생성할 수 있다. 또한 이 서명을 받은 검증자도 다음 식과 대리 서명 공개키를 검증할 수 있다.

$$\rho_i \equiv g^{\lambda_i} \pmod{p}$$

$$\equiv y_0^{e_0} y_1^{e_1} \cdots y_{i-1}^{e_{i-1}} y_i^{e_{i-1}} K_0 K_1 \cdots K_{i-1} \pmod{p}$$

5. 결론

대리서명 기법은 Mambo[1]~[2], KPW[3] 등에 의해서 제안이 되었으나 다단계 대리 서명 방식을 만족시키기에는 몇 가지 문제점이 있었다. 따라서 안전한 다단계 대리서명을 위해서는 원 서명자의 위임 부인을 방지하여 대리서명자를 보호할 수 있어야 하며, 원 서명자에게는 자신이 위임한 서명이 실제로 이루어진 상황을 알 수 있게 하여 원 서명자의 서명에 대해 보호할 수 있어야 한다.

Kim[5]에서 제시한 보증서(원 서명자 식별자ID, 대리서명자 ID, 위임기간 등)는 공개기관의 인증서 표준 방식을 따르지 않으므로 부인 방지 및 정보 보호 등의 책임을 사설기관이 져야 하며 다단계로 확장시 보증서 보관에 대한 문제점들이 발생할 수 있다. 위임인증서를 이용한 다단계 대리서명 방식은 이러한 발생 가능한 문제점 등을 해결하여, 보다 강력한 위임 부인봉쇄가 가능하게 된다.

제안한 방식은 위임 인증서에 원 서명자의 정보를 추가적으로 삽입하여 위임 인증서를 재구성함으로써 원 서명자와 대리서명자의 보호가 동시에 이루어지도록 설계되었으며, 기밀성, 인증, 부인봉쇄, 유효성, 안정

성, 원 서명자 확인 등의 보안 특성을 만족하여 기존의 대리서명이나 보증서를 이용한 대리서명 방식 보다 더 안전함을 보였다.

참고문헌

- [1] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature : Delegation of the power to sign message", IEICE Transaction on Fundamentals, vol. E79-A, no. 9, pp. 1338~1354, 1996.
- [2] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature for delegating signing operation", Proc. Third ACM Conf. on Computer and Communications Security, pp. 48~57, 1996.
- [3] S. Kim, S. Park and D. Won, "Proxy signatures, revisited", Proc. of ICICS'97, LNCS 1334, pp. 223~232, 1997.
- [4] S. Araki and K. Imamura, "An application of Mambo - Usuda - Okamoto Proxy Signature Schemes", Proc. of ISITA, 2000.
- [5] 김소진, 이명희, 최재귀, 박지환, "대리 서명 방식의 확장에 관한 연구", 한국멀티미디어학회춘계발표논문지, 제5권, 제1호, pp. 844~848, 2002.5.
- [6] 조상래, 이정연, 진승현, 김태성, "위임 인증서를 이용한 대리 서명 기술", 한국정보과학회추계발표논문지, 제29권, 제2호, pp. 676~678, 2002.10.
- [7] S. Tuecke, D. Engert, I. Foster, "Internet X.509 Public Key Infrastructure Proxy Certification Profile", Internet Draft draft-ietf-pkix-05.txt, Feb. 2003.