SPSS의 안전성 강화 및 대리은닉 서명 기법의 제안

김배완, 류종호, 심현정, 염흥열

순천향대학교 정보보호학과

Proxy Blind Signature based on improved SPSS

Kim-Baewan, Ryu-Jongho, Shim-Hyunjung, Youm-Heungyoul

Department of Information Security SoonChunHyang Univ.

요 약

대리 서명 방식은 전자서명 방식의 한 응용분야로써 1996년 Mambo[1]에 의하여 처음으로 제안되었으며, 이후 다양한 특성을 갖는 Schnorr 서명 기반 대리 서명들이 [2,3]에서 제안되었다. 특히 B.Lee[3]은 대리 서명키의 오용을 막을 수 있는 강한 대리 서명 기법(Strong Proxy Signature Scheme, SPSS)을 제시하였다. 그러나 이 기법에 대하여 [6]은 서명위조 공격에 안전하지 않음을 기술하였다. 본 논문에서는 이와 같은 공격을 피할 수 있도록 방법을 제시하면서 더불어 이를 응용한 대리은닉 서명(proxy blind signature)을 제안한다.

I 서론

대리 서명 방식은 원 서명자가 대리 서명자에게 자신의 서명권한을 위임하고 이후 대리 서명자가 원 서명자를 대신하여 서명 생성이 가능하도록 하는 전자서명 응용 기법이다[1]. 1996년 Mambo[1]에 의하여 처음으로 제안된 이후 다양한 특성을 갖는 대리 서명 기법이 제안된다[2,3]. [2]에서는 대리 서명에 보증기간(warrant) 개념 및 대리 서명자를 보호할 있는 특성을 제안하였고, SPSS[3]에서는 대리 서명키의 오용을 막을 수 있는 강한 대리 서명 기법을 제시하였다. 특히 SPSS는 Schnorr 서명을 기반으로 보증기간 및 원 서명자의 오용을 막을 수 있도록 설계하였으며 이에 대한 응용으로 대리 서명 기법에 은닉 서명 기법을 도입할 수 있음을 설명하였다.

[6]에서는 SPSS의 취약점을 제시한다. SPSS에서 원 서명자가 대리 서명자의 대리 서명문을 도청한 후 자신의 개인키 정보가 담겨 있는 부분을 없애 버린다면 이 대리 서명문은 오히려 대리 서명자 자신의 Schnorr 서명이 되어 버린다. 결과적으로 원 서명자에 의한 서명위조 공격에 대리 서명자가 노출되어 있음을 제시하였다.

은닉 서명(blind signature) 기법은 D.Chaum에 의해서 제안된 것으로 서명자가 원 메시지 내용을 보지 못한 상태에서 서명을 하는 방식이다[9]. 이는 마치 원 메시지 위에 묵지를 올려놓고 봉투에 넣어 서명자가 서명문 내용을 알지 못하는 상태에서 서명할 수 있도록 하는 서명 방식이다.

[3,7]에서는 대리 서명 기법에 은닉 서명 기법을 추가적으로 응용할 수 있음을 보였다. 이는 원 서명자가 은닉 서명을 수행하되 이를 대리 서명자에게 위임할 수 있는 서명 시스템으로 볼 수 있다. 이 같은 서명 시스템은 금융시스템에 있어 효율성을 개선할 수 있는 서명응용이라 할 수 있다.

본 논문에서는 SPSS의 취약점을 보완할 수 있는 개선된 대리 서명 기법을 제시한다. 더불어 이 서명 기법에 은닉 서명 기법을 도입하여 SPSS의 특성을 그대로 유지한 강한 대리은닉 서명 기법을 제시한다.

이와 같은 사항을 설명하기 위하여, 2장에서는 대리 서명 기법의 간략한 특징, SPSS, 그리고 이에 대한 서명위조 공격을 기술한다. 3장에서는 이와 같은 공격에 대항하기 위한 개선된 SPSS을 제시하며 동시에 이를 응용한 대리은닉 서명을 구성한다. 4장에서는 이에 대한 보안평가 및 성능 분석을 검증한 후 결론을 맺는다.

II SPSS 및 서명위조 공격

본 절에서는 SPSS와 이에 대한 서명위조 공격을 소개한다. 두 프로토콜의 설명에 앞서 서명의 기본이 되는 Schnorr 서명 기법을 설명한다.

2.1 Schnorr 서명 기법

[5]에서 소개된 Schnorr 서명은 다음의 절차를 따른다.

p와 q는 큰 소수이고 $q|\phi(p)$이다. 원시근 g는 위수가 q인 GF(p)중의 한 원소이며 유한 순환군 $G=\langle g\rangle$을 이룬다. $h:\{0,1\}^*\rightarrow Z_q$는 충돌회피성 해쉬함수이며 랜덤 오라클과 같이 동작된다고 가정한다. 여기에서 $k\ll\log_2 q$ 이고 $q<p$이다.

서명자 A는 자신의 개인키 $x_A\in Z_q^*$을 선택하고 이에 해당되는 공개키 $y_A\equiv g^{x_A} \bmod p$을 공개한다. 메시지 M에 서명하기 위하여 다음과 같은 절차를 따른다.

- 서명자는 $k\in_R Z_q^*$을 선택한 후 $r\equiv g^k \bmod p$, $e=h(M\|r)$, 그리고 $s\equiv x_A e+k \bmod q$을 계산한다.
- 서명자는 메시지 M과 이에 대한 서명문쌍 (s,r)을 수신자에게 전달한다.
- 수신자는 서명문의 정확성을 검증하기 위하여 $g^s \stackrel{?}{=} r y_A^e \bmod p$을 검증한 후 이를 받아 들인다.

램덤 오라클 모델에서 Schnorr 서명을 위조하는 것은 유한 순환부분군 G에서의 DLP(Discrete Logarithm Problem)과 동일한 확률을 갖는다. 이 사항은 [8]에 증명되어 있다.

2.2 강한 대리 서명 기법의 특성

대리 서명 방식은 원 서명자가 대리 서명자에게 자신의 서명권한을 위임하여 대리 서명자가 원 서명자를 대신하여 서명 생성이 가능하도록 하는 전자서명 응용 기법 중의 하나이다[1]. 대리 서명 기법은 Mambo, Usuda와 Okamoto[1]에 의해 소개된 이후, 위임강도에 따라 대리 서명 형태를 구분할 수 있도록 했으며 또한 대리 서명자를 보호하도록 제안되어 왔다[2,3,4].

강한 대리 서명의 기술을 위한 보안요구 사항들은 다음 사항을 내포하고 있어야 한다[3].

- 강한 위조방지 : 원 서명자로부터 위임 서명자로 지정된 대리 서명자가 원 서명자에 대한 대리 서명을 생성할 수는 있다. 그러나 원 서명자를 포함한 어떠한 제 삼자라도 대리 서명을 생성할 수 없어야 한다.
- 강한 확인성 : 누구라도 대리 서명으로부터 대리 서명자를 확인할 수 있어야 한다.
- 강한 부인방지 : 대리 서명자는 서명 이후에 누구에게도 유효한 서명을 생성한 사실을 부인할 수 없어야 한다.
- 남용방지 : 대리 서명자는 생성한 대리 서명을 정당하게 위임받지 않은 메시지나 다른 목적을 위해 사용할 수 없어야 한다.

2.3 SPSS[3]

본 절에서는 [3]에서 제안된 Schonor 서명 기반 강한 대리 서명 방식을 설명한다. 제안된 프로토콜의 참여자로는 원 서명자, 대리 서명자, 그리고 서명문을 수신하는 사용자로 구성된다. 서명 수행에 앞서 원 서명자 A는 자신의 개인키 x_A와 이에 대응되는 공개키 y_A을 소지하고, 대리 서명자 B 역시 자신의 개인키 x_B와 이에 대응되는 공개키 y_B을 소유한다. 공개키들은 모든 참여자들에게 공개된다.

- 대리 서명키의 생성

원 서명자 A는 유효기간이 포함된 메시지(warrant) M_w에 서명하기 위하여 Schnorr 서명을 이용한다. 대리 서명키를 생성하기 위하여 원 서명자 A는 $k_A\in_R Z_q^*$를 생성하고 $r_A=g^{k_A}$와 $e_A=h(M_w\|r_A)$, 그리고 $s_A=k_A+x_A e_A$를 계산한다. 원 서명자는 비밀스러운 통신채널을 통하여 서명문쌍 (r_A, s_A)와 보증기간 M_w를 대리 서명자 B에게 보낸다.

대리 서명자는 원 서명자로부터 받은 정보를 이용하여 $e_A=h(M_w\|r_A)$을 계산하고 서명정보가 정당한지 검증한다. 즉 $g^{s_A} \stackrel{?}{=} r_A y_A^{e_A}$를 비교한다.

만약 검증이 올바르다면, 대리 서명자는 대리 서명키 $x_P = x_B + s_A$을 획득하게 된다. 여기에서 대리 서명키에 대응되는 공개키로는 $y_P = g^{x_P}$가 된다.

◦ 대리 서명문의 생성

메시지 M에 대한 대리 서명문을 생성하기 위하여, 대리 서명자 B는 M_w이 포함된 Schnorr 서명을 생성한다. 메시지 M에 대한 대리 서명문쌍 (r_P, s_P)을 계산하기 위해서는 대리 서명키쌍 x_p와 y_P를 이용해야 한다. 정확한 대리 서명문은 (M, M_w, r_A, r_P, s_P)가 된다.

이를 계산하기 위하여 대리 서명자는 $k_P \in Z_q^*$를 선정하여 $r_P = g^{k_P}$, $e_P = h(M \| r_P)$, 그리고 $s_P = k_P + x_P e_P$를 생성한다.

◦ 대리 서명문의 검증

사용자는 대리 서명자로부터 받은 서명문을 검증하기 위하여 우선 다른 두 참여자들의 공개키 y_A와 y_B을 사전에 알고 있어야 한다. 사용자는 대리 서명자로부터 받은 정보를 이용하여 $e_A = h(M_w \| r_A)$와 $e_p = h(M \| r_p)$를 계산한 후, $g^{s_P} \stackrel{?}{=} r_P (y_B r_A y_A^{e_A})^{e_P}$을 검증한다. 위 검사가 통과된다면, 사용자는 원 서명자와 대리 서명 권한을 부여받은 대리 서명자가 서로 협력하여 서명문을 생성하여 주었음을 확신한다.

2.4. SPSS에 대한 서명위조 공격[6]

[6]에서는 원 서명자가 대리 서명자의 대리 서명문을 도청한 후 자신의 개인키 정보가 담겨 있는 부분을 없애 버린다면 이 대리 서명문을 오히려 대리 서명자 자신의 Schnorr 서명이 되어 버림을 제시하였다.

단계 1. 원 서명자 A는 대리 서명자 B가 사용자에게 보내는 대리 서명문 (M, M_w, r_A, r_P, s_P)을 도청한다.

단계 2. 원 서명자 A는 $s' = s_A e_P$를 생성한다. 여기에서 $e_P = h(M \| r_P)$

단계 3. $s_B = s_P - s' = k_P + x_B e_P$를 계산한 다음에 $r_B = r_P$가 되도록 한다

단계 4. 결과적으로 원 서명자 A는 메시지 M과 대리 서명자 자신이 생성한 서명문쌍 (r_B, s_B)을 얻을 수 있게 된다. 만일 B의 공개키를 이용하여 Schnorr 서명 검증식 $g^{s_B} \stackrel{?}{=} r_B y_B^{h(M \| r_B)}$을 통과 할 수 있다면, 이는 정확한 대리 서명자의 서명문이 된다. 결과적으로 원 서명자 A은 대리 서명자 B에게 서명위조 공격을 수행할 수 있게 된다.

III 개선된 SPSS의 제안 및 대리은닉 서명

3.1 개선된 SPSS

본 절에서는 2장에 제시된 공격에 저항하기 위한 개선된 SPSS을 제시하며 동시에 이를 응용한 대리은닉 서명을 구성한다. 기본 아이디어는 원 서명자 A가 s_P에서 자신의 서명성분 s_A을 삭제하지 못하도록 하는 것에 있다.

SPSS은 그대로 유지하되 다음 각 단계에서 몇 가지 사항을 수정한다.

◦ 대리 서명키의 생성 단계

$x_P = x_B + s_A$를 $x_P = x_B^{-1} s_A$로 대체한다. 여기에서 x_B^{-1}은 법 q에 대한 곱셈역원이다.

◦ 대리 서명문의 생성 단계

$r_P = g^{k_P}$를 $r_P = y_B^{k_P}$로 대체한다.

◦ 대리 서명문의 검증 단계

대리 서명문의 검증식 $g^{s_P} \stackrel{?}{=} r_P (y_B r_A y_A^{e_A})^{e_P}$를 $y_B^{s_P} \stackrel{?}{=} r_P (r_A y_A^{e_A})^{e_P}$로 대체한다.

◦ 보안 분석 : 개선된 SPSS에서 원 서명자 A가 $s_P = k_P + (x_P) e_P = k_P + (x_B^{-1} s_A) e_P$을 도청한다 하더라도, s_A 성분을 빼내는 것은 DLP와 동일한 문제이다. 왜냐하면 s_A를 빼내기 위해서는 x_B를 구해야 하기 때문이다. 즉 y_B에서 x_B를

원서명자 A (x_A, y_A)	대리 서명자 B (x_B, y_B, y_A)	사용자 (y_A, y_B, M)

대리 서명키 생성 단계			대리은닉 서명문 생성 단계		
$k_A \in_R Z_q^*$ $r_A \equiv g^{k_A} \pmod p$ $e_A = h(M_w \| r_A)$ $s_A \equiv k_A + x_A e_A$	M_w , (r_A, s_A) $\longrightarrow$		$k_P \in_R Z_q^*$ $\gcd(x_B, k_P) = 1$ $r_P \equiv y_B^{k_P} \pmod p$ $e_P = h(M_w \| r_P)$ $s_P \equiv k_P + x_P e_P$	M_w , (r_A, r_P) $\longrightarrow$	
		$e_A = h(M_w \| r_A)$ $g^{s_A} \stackrel{?}{=} r_A y_A^{e_A}$ 대리 서명자 B의 대리 서명키 x_P	$s_P = k_P + x_P e_P$	e_P $\longleftarrow$	$\alpha, \beta \in_R Z_q^*$ $e_A = h(M_w \| r_A)$ $r' \equiv r_P y_B^{-\alpha} (r_A y_A^{e_A})^{-\beta}$ $\equiv r_P y_B^{-\alpha} y_P^{-\beta}$ $e' = h(M \| r')$ $e_P \equiv e' - \beta \pmod q$
		$x_P \equiv x_B^{-1} s_A$ $y_P \equiv y_B^{x_P}$		s_P $\longrightarrow$	$s' \equiv s_P - \alpha$ $y_B^{s'} \stackrel{?}{=} r' (r_A y_A^{e_A})^{e'}$

그림 1. SPSS 기반 대리은닉 서명

구하는 DLP가 된다. 따라서 원 서명자 A는 대리 서명자 B의 서명문을 위조하는 것은 계산적으로 어려운 문제이다.

3.2 은닉 서명(blind signature)

은닉 서명 방식은 전자현금(electronic cash)이나 전자투표(electronic vote)와 같은 개인의 프라이버시를 요구하는 응용분야에서 사용된다. 이를 만족시키기 위해 1982년 Chaum[9]에 의해 처음으로 RSA 기반의 은닉 서명 개념이 제안되었다. 기본적으로 사용자 B는 자신의 메시지 M을 서명자 A에게 보여주지 않으면서도 서명을 받아낸다. 은닉 서명은 다음과 같은 절차로 이루어진다.

- 서명자 A가 메시지 M에 대한 은닉 서명을 생성하기 위하여, 우선 $k \in_R Z_q^*$를 생성하고 $r = g^k$을 계산한 다음 r을 사용자 B에게 전달한다.
- 사용자 B는 $\alpha, \beta \in_R Z_q^*$ 를 랜덤하게 생성하고 $r' = r g^{-\alpha} y^{-\beta}$, $e' = h(M \| r')$, $e = e' - \beta$를 계산한 후, e를 서명자 A에게 전달한다.
- 서명자 A는 $s = xe + k$를 계산한 후, 이를 사용자 B에게 되돌려 준다.
- e를 수신한 사용자 B는 $s' \equiv s - \alpha \pmod q$를 구한 다음, 최종적으로 메시지 M에 대한 은닉 서명문 쌍(s', e')을 얻게 된다.
- 이후 $d' = g^{s'} y^{-e'}$을 구하고 $e' \stackrel{?}{=} h(M \| d')$을 검증함으로써 서명문에 대한 확신을 갖게된다.

3.3 대리은닉 서명

대리은닉 서명의 목적은 원 서명자로부터 위임받은 대리 서명자가 서명문의 내용은 알지 못한 상태에서 대리 서명을 할 수 있도록 하는 것이다. 대리 서명자는 정확하게 위임받은 서명정보를 이용하여 대리은닉 서명을 한다[3,7].

본 절에서는 개선된 SPSS를 이용한 대리은닉 서명을 제안한다. 프로토콜은 대리 서명을 위조할 수 없으며, 대리 서명자가 보호되도록 설계된

다. 또한 원 서명자는 대리 서명자에게 위임 부인 방지하도록 설계된다. 그림 1은 제안된 대리은닉 서명을 도시한 것이다. 그림에서 최상단 부분의 괄호 영역은 참여자의 사전지식이다.

그림 1의 프로토콜 수행결과를 통하여 사용자는 메시지 M에 대한 서명문 (r', s', r_A, M_w)을 얻게 된다.

Ⅳ 보안 분석

제안된 대리은닉 서명에 대한 보안은 다음과 같다.

(1) 대리 서명 위조 불가능

대리 서명자의 대리 서명키는 $x_P = x_B^{-1} s_A$ 로 구성되기 때문에 원 서명자를 포함한 어떠한 제 3 자가 임의의 대리 서명을 생성하지 못한다. 만일 $s_p = k_P + x_B^{-1} s_A e_P$를 알아냈다고 하더라고 공격자가 x_B를 알아내는 것은 DLP를 풀어내는 것만큼 어렵다.

(2) 원 서명자에 의한 대리 서명자의 서명위조

$s_P = k_P + (x_P)e_P = k_P + (x_B^{-1} s_A)e_P$을 원 서명자 A가 도청한다 하더라도, s_A 성분을 빼내는 것은 DLP와 동일한 문제이다. 따라서 위조 서명문 $k_P + x_B e_P$를 구하는 것 또한 DLP를 풀어내는 것만큼 어렵기 때문에 대리 서명자의 서명문을 위조하는 것은 계산적으로 상당히 어렵다.

(3) 원 서명자의 부인방지

사용자가 대리 서명자로 받은 서명문을 검증할 때의 검증식은 $y_B^{s'} = r'(r_A y_A^{e_A})^{e'}$와 같다. 따라서 대리 서명문이 원 서명자의 공개키 y_A가 삽입된 검증식을 통과된다면, 원 서명자는 대리 서명자에게 서명 위임한 것을 부인할 수 없고 또한 사용자는 대리 서명자가 원 서명자로부터 위임을 받아 대신 서명하였다는 것을 확신 할 수 있다.

(4) 효율성 비교

다음은 각 프로토콜의 연산을 비교한 것이다. 지수승 연산 횟수는 효율성을 위하여 다중 병렬 멱승법(simultaneous multiple exponentiation)[10]을 취한다

횟수	해쉬			지수승			난수 생성		
	O	P	U	O	P	U	O	P	U
[7]	-	-	2	2	2	1	1	1	2
[3]	1	3	2	1	3	1	1	1	-
제안된 프로토콜	1	1	3	1	3	3	1	1	1

여기에서 O는 원 서명자이고, P는 대리 서명자, 그리고 U는 사용자이다.

Ⅴ. 결론

본 논문에서는 SPSS의 취약점을 보완하고 이를 토대로 대리은닉 서명을 제안하였다. 개선된 SPSS는 원 서명자의 서명위조 공격에 강한 저항성을 유지하며, SPSS에 강한 대리서명 기법의 특성을 그대로 유지한다.

개선된 대리 서명을 이용한 대리 은닉 서명은 대리 서명자가 정확하게 위임받은 서명정보를 이용하여 대리은닉 서명을 수행하기 때문에 대리 서명을 위조 할 수 없고, 사용자는 대리 서명자가 원 서명자로부터 위임을 받아 대신 서명하였다는 것을 확신 할 수 있다.

제안된 대리은닉 서명 기법은 전자 현금을 사용하는 전자 뱅킹, 기업대 기업간 전자상거래 등 사용자들의 개인정보를 보호해야하는 분야에 다양하게 적용 가능 할 수 있다.

참고 문헌

[1] M.Mambo, K.Usuda, E.Okamoto, "Proxy signature : Delegation of the power to sign message," IEICE Trans. Fundamentals Vol. E79-A, No.9, p. 1338-1353. 1996

[2] Seungjoo Kim, SangJoon Park, Dongho Won, "Proxy Signatures, Revisited," Proc. of International Conference on Information and Communications Security (ICISC'97) p. 223-232

[3] Byoungcheon Lee, Heesun Kim, Kwangjo Kim, "Strong Proxy Signature and its Applications," The 2001 Symposium on Cryptography and Information Security (SCIS 2001)
[4] Javier Herranz, German Saez, "Full Distributed Proxy Signature Schemes," the proceedings of Financial Cryptography Conference, 2003. http://eprint.iacr.org/2002/051/
[5] C.P.Schnorr, "Efficient signature generation by smart cards," Journal of Cryptology Vol. 4, p. 161-171, 1991
[6] Zheng Dong, Shengli Liu & kefei Chen, "Cryptanalysis of B.Lee-S.Kim-K.Kim Proxy Signature," http://eprint.iacr.org/2003/200/
[7] Sunder Lal, Amit Kumar Awasthi, "Proxy Blind Signature Scheme," http://eprint.iacr.org/2003/072/
[8] D.Pointcheval and J.Stern, "Security proofs for signature schemes," Advances in Cryptology Eurocrypto'96, LNCS 1070, p. 387-398
[9] D.Chaum, "Blind signature for untraceable payments," Advances in Cryptology Crypto'82
[10] A.Menezes, P.van Oorschot, S.Vanston, "Handbook of applied cryptography," CRC Press, Inc., pp 618, 1997