개선된 Xue-Cao threshold 대리서명 기법의 안전성

박제홍, 박상우
국가보안기술연구소

Security of the revised Xue-Cao threshold proxy signature scheme

Je Hong Park, Sangwoo Park
National Security Research Institute.

요 약

다중 사용자 환경에서 안전한 대리서명을 설계하는 연구의 하나로, threshold 서명 방식을 대리서명에 적용한 threshold 대리서명 기법들이 최근 많이 제안되고 있다. Xue와 Cao가 2004년 발표한 threshold 대리서명 기법은 Hsu-Wu 자체인증 공개키 방식 (Self-certified public key)을 기반으로 설계된 것으로 WISA 2005, CISC 2005, ICCSA 2006에서 각각 다른 취약성이 밝혀진 바 있다. 특히 CISC 2005, ICCSA 2006에서는 각각의 공격방법에 내성을 가질 수 있도록 Xue-Cao 기법을 개선하는 방안을 같이 제시하였다. 본 논문에서는 이러한 개선안이 적용된 Xue-Cao 기법에 대해 두 가지 종류의 원서명자 위조 공격이 가능함을 보인다. 하나는 Hsu-Wu 자체인증 공개키 방식의 취약성을 이용하는 것이고 다른 하나는 Xue-Cao 기법의 서명 생성 방식의 취약성에 기반한 것이다. 이러한 공격을 통해 개선된 Xue-Cao 기법 또한 대리자 보호, 부인방지와 같은 안전성 조건을 만족하지 않음을 확인한다.

I. 서론

대리서명(Proxy Signature)은 두 사용자 사이의 권한위임을 통해 대리서명자가 원서명자를 대신하여 유효한 서명을 생성하는 방법이다. Mambo 등 [7]이 대리서명의 개념을 처음 소개한 이후 다양한 대리서명 기법이 제안되고 있으며, 특히 blind 서명, threshold 서명, multi 서명과 같은 개념을 도입하여 기존 대리서명의 성질을 확장한 기법 또한 제안되고 있다.

Threshold 대리서명은 1997년 Zhang [13]과 Kim 등 [5]이 독립적으로 제안하였으며 이후 지금까지 다양한 방식이 제안되고 있다 [3,4,12]. 일반적으로 (t,n)-threshold 대리서명은 원서명자가 자신의 서명권한을 n명의 대리서명자로 구성된 그룹에 위임하여 t명 이상의 대리서명자가 서로 협력하여 대리서명을 생성한다. 이때, 위임받은 대리서명자만이 유효한 대리서명을 생성할 수 있으며, 원서명자라도 대리서명을 생성할 수 없어야 한다는 기본적인 대리서명이 가지는 대리자 보호(Proxy Protected), 부인방지(Nonrepudiation) 성질과 함께, t명 이상의 대리서명자의 협력에 의해서만 유효한 대리서명을 생성할 수 있는 threshold 서명의 위조방지(Unforgeability) 성질을 같이 제공해야 한다.

2004년 Xue와 Cao [11]는 Hsu-Wu 자체인증 공개키 방식(Self-certified public key) [2]을 적용한 threshold 대리서명 기법 (이하 XC 기법)을 제안하였지만, WISA 2005 [8], CISC 2005 [1], ICCSA 2006 [6]에서 각기 다른 형태의 취약성이 제시되었다. 논문 [1]에서는 악의를 가진 대리서명자가 임의의 메시지에 대한 대리서명을 위조할 수 있음을 보였고, 논문 [6]에서는 악의를 가진 원서명자가 주어진 유효한 대리서명을 이용하여 다른 유효한 대리서명을 위조할 수 있음을 보였다.

논문 [1,6]에서는 자신들이 제안한 공격에 내성을 가질 수 있도록 XC 기법에 대한 수정안을 제시하였다. 하지만 본 논문에서는 개선된

XC 기법에 대해서도 WISA 2005에서 제시한 바 있는 Hsu-Wu 자체인증 공개키 방식의 취약성에 기반한 원서명자의 위조 공격이 가능함을 보이고, 또한 최근 Yang 등이 제안한 threshold 대리서명 기법 [12]에 대해 Shao 등이 제안한 공격방법 [9]이 개선된 XC 기법에도 그대로 적용됨을 보인다.

본문의 구성은 다음과 같다. II 절에서는 개선된 XC 기법에 대해 간략하게 살펴보고, III 절에서는 두 가지 공격 방법을 제시한다. IV 절에서는 결론을 맺는다.

II. Xue-Cao 대리서명 기법

XC 기법은 Hsu-Wu가 제안한 이산대수 기반의 자체인증 공개키 [2]를 사용하며, 서명 생성과 검증은 Yang 등이 제안한 대리서명 기법 (이하 YTH 기법)[12]과 동일하다. Hsu-Wu 자체인증 공개키 방식은 사용자 등록을 관리하는 시스템 관리자 (SA) 가 사용자 등록 (registration)과정을 통해 사용자의 공개키를 정해준다. XC 기법은 이러한 사용자 키 등록 과정에 이어 대리서명 키를 생성하는 대리 비밀분산 생성 (proxy secret share generation), 그리고 대리서명 생성 (proxy signature generation)과 대리서명 검증 (proxy signature verification)의 네 단계로 구성된다. 아래에서는 논문 [1,6]의 제안에 의해 개선된 XC 기법을 소개한다.

먼저 p와 q를 두 큰 소수라 하자. 여기에서 $q \mid (p-1)$이고 g는 F_p상의 위수가 q인 부분군의 생성자 (generator)이다. 그리고 안전한 일방향 해쉬함수 $H_1 : \{0,1\}^* \rightarrow Z_q^*$와 $H_2 : \{0,1\}^* \rightarrow F_p^*$를 가정하자.[1] 파라미터 (p,q,g)와 H_1, H_2는 공개된다. ID_i는 사용자 U_i에 대한 개인식별정보 (identity)이며 Z_q^*의 원소를 사용한다. SA의 개인키와 공개키는 각각 γ와 β로 $\gamma \in Z_q^*$이고 $\beta = g^{\gamma} \bmod p$이다. 서명기법의 각 단계는 다음과 같다.

· **등록**: 각 사용자 U_i는 임의로 $t_i \in Z_q^*$를 선택하여 $v_i = g^{H_1(t_i \| ID_i)} \bmod p$를 계산하고 (v_i, ID_i)를 SA에게 보낸다. SA는 임의로 $z_i \in Z_q^*$를 선택하고

$$y_i = v_i H_2(ID_i)^{-1} g^{z_i} \bmod p \quad (1)$$
$$e_i = z_i + H_1(y_i \| ID_i)\gamma \bmod q,$$

를 계산하여 (y_i, e_i)를 U_i에게 보낸다. 그러면 U_i는 $x_i = e_i + H_1(t_i \| ID_i) \bmod q$를 계산하고 그 유효성을 다음 식을 통해 확인한다.

$$\beta^{H_1(y_i \| ID_i)} H_2(ID_i) y_i = g^{x_i} \bmod p \quad (2)$$

이 식이 성립하면 U_i는 (x_i, y_i)를 자신의 개인키와 공개키 쌍으로 받는다. SA는 등록과정을 완료한 후, U_i의 공개키 y_i를 공시한다.

· **대리 비밀분산 생성**: U_o를 원서명자, 그리고 $G = \{U_1, \cdots, U_n\}$를 n명의 대리서명자 U_i로 구성된 그룹이라 하자. 그리고 m_w는 원서명자와 대리서명자들의 개인식별정보, 위임기간, threshold 값 t 등의 정보를 포함하는 위임장 (warrant)이라 하자. 원서명자는 자신의 서명 권한을 위임하기 위해 다음의 절차를 수행한다.

Step 1: 먼저 임의로 $k \in Z_q^*$를 선택하고, 다음 값을 계산한다.

$$K = g^k \bmod p, \quad \sigma = H_1(m_w \| K) x_o + kK \bmod q.$$

Step 2: 보안경로를 통해 $(m_w, (K, \sigma))$를 각 대리서명자에게 전송한다. 각 대리서명자는 다음 식을 확인함으로써 σ의 유효성을 확인한다.

$$g^{\sigma} = K^K (\beta^{H_1(y_o \| ID_o)} H_2(ID_o) y_o)^{H_1(m_w \| K)} \bmod p.$$

· **대리서명의 생성**: $D = \{U_1, \cdots, U_t\}$를 G에서 실제 서명에 참여하는 대리서명자라 하고 ASID를 D에 속하는 모든 사용자의 개인식별정보의 집합이라 하자. D에 속하는 모든 사용자는 m에 대한 대리서명을 다음과 같은 절차에 따라 생성한다.

Step 1: 각 사용자 U_i는 $k_i \in Z_q^*$를 임의로 선택하고 $R_i = g^{k_i} \bmod p$를 계산하고, 모든 사용자가 동시에 공개한다.

Step 2: 다른 사용자들로부터 R_j를 얻은 다음, 각 사용자 U_i는 다음을 계산한다.

$$R = \prod_{i=1}^{t} R_i \bmod p$$
$$s_i = k_i R + (\sigma t^{-1} + x_i) H_1(m \| R \| ASID) \bmod q \quad (3)$$

1) 논문 [11]에서는 H_1과 H_2의 구분 없이 하나의 일반적인 일방향 해쉬함수를 이용하여 표현하였지만, 본 논문에서는 그 역할을 구분하기 위하여 두 개의 해쉬함수로 표현하였다.

그리고 (K,R,s_i)을 지정된 대표자 (designated clerk)에게 전송한다.

Step 3: 각 사용자로부터 s_i를 받은 대표자는 다음을 확인하여 유효성을 검증한다.

$$g^{s_i} = R_i^{R}((K^{K}(\beta^{H_1(y_o\|ID_o)}H_2(ID_o)y_o)^{H_1(m_w\|K)})^{t^{-1}}$$
$$\beta^{H_1(y_i\|ID_i)}H_2(ID_i)y_i)^{H_1(m\|R\|ASID)} \bmod p.$$

만일 유효하다면, (R_i,s_i)는 m에 대한 U_i의 유효한 개별 대리서명 (individual proxy signature)이다. 만일 모든 i $(1 \le i \le t)$에 대해 (R_i,s_i)가 검증되면, 대표자는 $S=\sum_{i=1}^{t} s_i \bmod q$를 계산하고 m에 대한 대리서명으로 $(ASID,\ m_w,\ K,\ (R,\ S))$을 제시한다.

· **대리서명의 검증**: 메시지 m에 대한 대리서명 $(ASID,\ m_w,\ K,\ (R,\ S))$을 받은 검증자는 m_w에서 원서명자의 개인식별정보와 대리서명자 그룹을 확인하고 ASID로부터 실제 서명자들의 개인식별정보, $|ASID| \ge t$를 확인한다. 이어서 SA나 대리서명자 그룹으로부터 필요한 공개키를 확보하여 다음 식을 통해 서명의 유효성을 확인한다.

$$g^{S} = R^{R}[(K^{K}\beta^{H_1(y_o\|ID_o)H_1(m_w\|K)+\sum_{i=1}^{t}H_1(y_i\|ID_i)} \quad (4)$$
$$(H_2(ID_o)y_o)^{H_1(m_w\|K)}$$
$$\prod_{i=1}^{t}(H_2(ID_i)y_i)]^{H_1(m\|R\|ASID)} \bmod p.$$

참고로 XC 기법에 대해 논문 [1,6]에서 제안한 수정 방안은 다음과 같다.

1. $H_1(m_w)$을 $H_1(m_w\|K)$으로 바꿀 것
2. $H_1(m\|ASID)$를 $H_1(m\|R\|ASID)$으로 바꿀 것
3. 대리서명 생성 시 Step 1에서 각 사용자는 R_i를 동시에 공개한다.

III. 안전성 분석

본 절에서는 개선된 XC 기법에 대한 두 가지 형태의 원서명자 위조 공격을 소개한다. 한 가지는 Hsu-Wu 자체인증 공개키 방식의 취약성에 기반한 것으로 WISA 2005 [8]에서 소개된 바 있다. 다른 공격의 경우 XC 기법의 서명 생성/검증 과정이 YTH 기법 [12]과 일치하는 것에 기반하여, YTH 기법에 대한 Shao 등의 공격 방법 [9]을 적용한 것이다. 우선 첫 번째 공격 방법은 다음과 같다.

대리서명자 그룹을 $G=\{U_1,\cdots,U_n\}$라 가정하고, 위조서명의 실제 서명자로 위장할 G의 구성원 $\{U_1,\cdots,U_r\}$의 모든 개인식별정보들의 집합을 ASID라 하자. G의 각 구성원 U_i $(i=1,\cdots,n)$는 등록 과정을 거쳐, 식 (2)의 관계를 만족하는 개인키/공개키 쌍 (x_i,y_i)을 갖는다고 가정하자. 메시지 m에 대해, 원서명자는 임의로 $t_o,\ k \in Z_q^*$를 선택하고 각 i $(1 \le i \le r)$에 대해 $k_i \in Z_q^*$를 선택한 후,

$$K=g^{k} \bmod p,\ R_i=g^{k_i} \bmod p,\ R=\prod_{i=1}^{r} R_i \bmod p,$$

를 계산하고 $\alpha=H_1(m_w\|K)^{-1}$로 둔다. 이때, m_w는 원서명자가 위조한 위임장이다.

위조된 서명이 ASID에 의해 서명된 것처럼 보이게 하기 위해, 원서명자는 등록단계에서 SA를 다음과 같이 속인다. 먼저, 원서명자는

$$v=g^{H_1(t_o\|ID_o)}(\beta^{\sum_{i=1}^{r}H_1(y_i\|ID_i)}\prod_{i=1}^{r}(H_2(ID_i)y_i))^{-\alpha} \bmod p$$

를 계산한 후, (v,ID_o)를 SA에게 보낸다. SA는 등록 과정의 절차에 따라 $z \in Z_q^*$를 임의로 선택하고,

$$y_o=vH_2(ID_o)^{-1}g^{z} \bmod p,\ e=z+H_1(t_o\|ID_o)\gamma \bmod q$$

를 계산한 후, (y_o,e)를 원서명자에게 반환한다. 원서명자는 $x_0=e+H_1(t_o\|ID_o) \bmod q$를 계산하고,

$$\beta^{H_1(y_o\|ID_o)}H_2(ID_o)y_o(\beta^{\sum_{i=1}^{r}H_1(y_i\|ID_i)}\prod_{i=1}^{r}H_2(ID_i)y_i)^{\alpha}=g^{x_o} \bmod p$$

이 성립하면, (x_o,y_o)를 자신의 개인키/공개키 쌍으로 받아들인다. 이 과정은 SA가 식 (1)의 계산을 정확하게 수행한 것인지 원서명자가 확인하는 것이다. 이러한 과정이 끝나면 SA는 U_o의 공개키 y_o를 공시한다. 이제 원서명자는

$$S=R\sum k_i+(x_oH_1(m_w\|K)+kK)H_1(m\|R\|ASID) \bmod q$$

를 계산하고 메시지 m에 대한 대리서명으로 $(ASID,\ m_w,\ K,\ (R,\ S))$를 제시한다. 검증자는 식 (4)를 계산하여 S의 유효성을 검증하게 된다. 즉, S는 메시지 m에 대해 원서명자가 $ASID$의 구성원들에 서명권한을 위임하여 생성한 것으로 위조된 threshold 대리서명이다.

이러한 공격은 등록 과정에서 SA가 사용자로부터

정보를 받아 검증 없이 키 생성에 필요한 값만 계산하여 반환하는 데에서 비롯된 것이다. 이러한 구조에서는 공격자가 원하는 형태의 키를 얻기 위해 등록 과정에서 처음 전송 정보를 조작하는 것이 가능하다.

이제 두 번째 공격 방법을 살펴본다. 대리서명 생성 단계에서 각 사용자는 식 (3)을 계산한다.

$$s_i = k_i K + (\sigma t^{-1} + x_i) H_1(m \| R \| ASID)$$
$$= k_i K + x_i H_1(m \| R \| ASID) + \sigma t^{-1} H_1(m \| R \| ASID) \bmod q.$$

악의를 가진 원서명자는 임의의 값 $k' \in Z_q^*$를 선택한 후, 위조한 위임장 m_w에 대해

$$K' = g^{k'} \bmod p,\ \sigma' = k' K' + x_o H_1(m_w \| K') \bmod q$$

를 계산한다. 그리고 주어진 유효한 대리서명 $(ASID,\ m_w,\ K,\ (R,S))$를 사용하여 다음을 계산한다.

$$S' = S - (\sigma - \sigma') H_1(m \| R \| ASID) \bmod q$$

그러면 식 (4)의 계산을 통해 S'가 유효함을 확인할 수 있다. 이러한 공격을 통해 원서명자는 실제 대리서명자를 변경하는 것은 불가능해도 위임기간과 같은 위임장의 주요 내용을 변경하여 서명을 위조하는 것이 가능하다.

IV. 결론

본 논문에서는 개선된 Xue-Cao threshold 대리서명 기법이 두 가지 종류의 원서명자 위조 공격에 취약함을 보였다. 한 가지 공격은 서명 기법이 사용하는 자체인증 공개키 생성 방식의 취약성의 취약성에서 비롯한 것으로 원사용자는 시스템 관리자를 속임으로써 주어진 메시지에 대한 서명을 위조할 수 있음을 보인다. 다른 하나는 주어진 유효한 대리서명을 이용하여 원서명자가 위임장을 위조, 이에 대한 새로운 서명을 생성하는 것이 가능함을 보였다.

[참고문헌]

[1] L. Guo, G. Wang and F. Bao. On the security of a threshold proxy signature scheme using self-certified public keys. Proc. of the SKLOIS conference on information security and cryptology - CISC 2005.

[2] C.-L. Hsu and T.-S. Wu. Efficient proxy signature schemes using self-certified public keys. Appl. Math. Comput., vol. 152(3):807-820 (2004).

[3] C.-L. Hsu and T.-S. Wu. Self-certified threshold proxy signature schemes with message recovery, nonrepudiation, and traceability. Appl. Math. Comput., vol. 164(1):201-225 (2005).

[4] C.-L. Hsu and T.-S. Wu. Efficient nonrepudiable threshold proxy signature scheme with known signers against the collusion attack. Appl. Math. Comput., vol. 168(1):305-319 (2005).

[5] S. Kim, S. Park and D. Won. Proxy signatures, revisited. Proc. of ICICS'97, LNCS 1334, pp. 223-232, 1997.

[6] J. Lu. Security weaknesses in two proxy signature schemes. Proc. of ICCSA 2006, LNCS 3982, pp. 466-475, 2006.

[7] M. Mambo, K. Usuda and E. Okamoto. Proxy signatures for delegating signing operation. Proc. of ACM CCS'96, pp. 48-57, 1996.

[8] J.H. Park, B.G. Kang and S. Park. Cryptanalysis of some group-oriented proxy signature schemes. Proc. of WISA 2005, LNCS 3786, pp. 10-24, 2006.

[9] J. Shao, Z. Cao and R. Lu. Improvement of Yang et al.'s threshold proxy signature scheme. J. Syst. Software, to appear.

[10] Z. Shao. Improvement of efficient proxy signature schemes using self-certified public keys. Appl. Math. Comput., vol. 168(1):222-234 (2005).

[11] Q. Xue and Z. Cao. A threshold proxy signature scheme using self-certified public keys. Proc. of ISPA 2004, LNCS 3358, pp. 715-724, 2004.

[12] C.-Y. Yang, S.-F. Tzeng and M.-S. Hwang. On the efficiency of nonrepudiable threshold proxy signatures with known signers. J. Syst. Software, vol. 73(3):507-514 (2004).

[13] K. Zhang. Threshold proxy signature schemes. Proc. of ISW'97, LNCS 1396, pp. 282--290, 1997.