2005 WSEAS Int. Conf. on DYNAMICAL SYSTEMS and CONTROL, Venice, Italy, November 2-4, 2005 (pp559-562)

Improvement of a Nominative Proxy Signature Scheme for Mobile Communication

KEON-JIK LEE[1], BYEONG-JIK LEE[2] and JEONG-HOON LEE[1]
Dept. of Electrical&Computer Engineering, Kangwon National University, Chuncheon, KOREA[1]
Dept. of Computer Engineering, Kyungpook National University, Daegu, KOREA[2]

Abstract: - Recently, Seo and Lee proposed a modification to the Park and Lee's nominative proxy signature scheme for mobile communication such that the original signer enables a proxy signer to nominate the verifier. However, the original signer can generate a valid nominative proxy signature without the proxy signer's knowing. In this paper, we show that Seo and Lee's modification is insecure against the original signer's forgery attack, and then propose an improved scheme to repair the security flaw.

Key-Words: - authentication, digital signature, discrete logarithm

1 Introduction

Digital signature confirms that the document originated from the signer and has not been altered. That is, it allows only one entity to sign messages in such a way that any receiver can verify the validity of the obtained signatures, but no one can forge signatures at will. In 1996, Mambo *et al.* [1] proposed the concept of the proxy signature scheme which enables a proxy signer to sign messages on behalf of the original signer. Delegating the signature power of the original signer to a proxy signer has been shown to be useful in many cases. Based on the delegation type, they classified proxy signatures as full delegation, partial delegation, and delegation by warrant. In full delegation, the original signer gives his secret key to the proxy signer, so the proxy signer has the same signature power as the original signer. But this is obviously not practical in most circumstances. In partial delegation, the proxy signature key is generated by the original signer and proxy signer. However, this does not set limits to the signature power of the proxy signer. This problem is solved by using a warrant. In delegation by warrant, the original signer issues the warrant which defines the relative rights and information between the original signer and proxy signer, what kinds of messages are delegated, and valid period of delegation, etc. When verifying the signature, the warrant is used as a part of verification information for the verifier. Among them, the partial delegation by warrant scheme is an issue of considerable practical significance and deserves a special notice.

Furthermore, due to its importance, many variations of proxy signature scheme have been proposed [2–7]. In 2001, Park and Lee [6] proposed the nominative proxy signature scheme for mobile communication which enables a proxy signer to nominate the verifier (nominee) and only the nominated verifier can verify the nominative proxy signature. Unfortunately, Seo and Lee [7] pointed out that Park and Lee's scheme is vulnerable to the original signer's forgery attack and proposed a new scheme to enhance Park and Lee's scheme and claimed that their scheme can withstand this attack. In this paper, we will review the scheme proposed by Seo and Lee and show that Seo and Lee's scheme still suffers from the original signer's forgery attack. Then, we will further propose an improved scheme and analyze the security.

2 Review of Seo and Lee's scheme

There are three communicating parties in the scheme: the original signer O, the proxy signer P, and the verifier V. Some notations are defined as follows:

- p, q large prime number with $q \mid (p-1)$
- g an element of order q in Z_p^*
- $h(\ )$ be a secure one-way hash function
- M a message
- T a time stamp
- W a warrant which contains the identities of the original signer and proxy signer and valid period of delegation, etc

- X_U the private key of user U
- Y_U the public key of user U, where $Y_U = g^{X_U} \bmod p$

Seo and Lee's scheme consists of three phases: the original signer phase, the proxy signer phase, and the verifier phase. Detailed description of each phase is given below.

Original Signer Phase

The original signer O generates a delegation key by using his private key.

Step 1: O selects $r_0 \in_R Z_q^*$ and computes $K_O = g^{r0} \bmod p$.

Step 2: O computes $e = h(W, T, K_O)$ and $S_O = X_O e + r_0 K_O \bmod q$, and then sends (W, T, K_O, S_O) to P. This phase is depicted as Fig. 1.

O $\xrightarrow{(W, T, K_O, S_O)}$ **P**

1. $r_0 \in_R Z_q^*$
   $K_O = g^{r_0} \bmod p$
2. $e = h(W, T, K_O)$
   $S_O = X_O e + r_0 K_O \bmod q$

Fig. 1 Original signer phase

Proxy Signer Phase

The proxy signer P generates the nominative proxy signature by using his private key, the delegation key and the nominee V's public key. The proxy signer phase runs as follows.

Step 1: P computes $e = h(W, T, K_O)$ and accepts (W, T, K_O, S_O) if $g^{S_O} = Y_O{}^e K_O{}^{K_O} \bmod p$ holds.

Step 2: P computes the proxy signature key $S_P = S_O + X_P K_O \bmod q$.

Step 3: P selects $r_1, r_2 \in_R Z_q^*$ and computes $K_P = g^{r_2 - r_1} \bmod p$, $D = Y_V{}^{r_2} \bmod p$, $E = h(Y_V, K_P, D, M, W)$, and $S = r_1 - S_P E \bmod q$. Next, P sends the nominative proxy signature $(M, Y_V, W, T, K_O, K_P, D, S)$ to V. We depict this phase as Fig. 2.

Verifier Phase

The verifier (nominee) V verifies the acquired nominative proxy signature by using his private key, the original signer's public key and the proxy signer's public key. The verification scenario is described as follows.

Step 1: V computes $e = h(W, T, K_O)$ and $E = h(Y_V, K_P, D, M, W)$.

Step 2: V accepts $(M, Y_V, W, T, K_O, K_P, D, S)$ as the nominative proxy signature if $(g^S(Y_O{}^e(Y_P K_O)^{K_O})^E K_P)^{X_V} = D \bmod p$ holds. This phase is depicted as Fig. 2.

P $\xrightarrow{(M, Y_V, W, T, K_O, K_P, D, S)}$ **V**

P:

1. $e = h(W, T, K_O)$
   $g^{S_O} = Y_O{}^e K_O{}^{K_O} \bmod p$
2. $S_P \stackrel{?}{=} S_O + X_P K_O \bmod q$
3. $r_1, r_2 \in_R Z_q^*$
   $K_P = g^{r_2 - r_1} \bmod p$
   $D = Y_V{}^{r_2} \bmod p$
   $E = h(Y_V, K_P, D, M, W)$
   $S = r_1 - S_P E \bmod q$

V:

1. $e = h(W, T, K_O)$
   $E = h(Y_V, K_P, D, M, W)$
2. $(g^S(Y_O{}^e(Y_P K_O)^{K_O})^E K_P)^{X_V} \stackrel{?}{=} D \bmod p$

Fig. 2 Proxy signer phase and verifier phase

Note that V's private key X_V is used in Step 2 of verifier phase. This means that only the nominee V can verify the validity of the nominative proxy signature. The correctness of Step 2 verification is described as follows:

$$\begin{aligned}
&(g^S(Y_O{}^e(Y_P K_O)^{K_O})^E K_P)^{X_V} \bmod p \\
&= (g^{r_1 - S_P E}(g^{X_O e}(g^{X_P} g^{r_0})^{K_O})^E g^{r_2 - r_1})^{X_V} \bmod p \\
&= (g^{r_1 - S_P E}(g^{X_O e + X_P K_O + r_0 K_O})^E g^{r_2 - r_1})^{X_V} \bmod p \\
&= (g^{r_1 - S_P E} g^{S_P E} g^{r_2 - r_1})^{X_V} \bmod p \\
&= (g^{r_2})^{X_V} \bmod p \\
&= D \bmod p
\end{aligned}$$

3 Cryptanalysis and Improvement

In this section, we show that Seo and Lee's nominative proxy signature scheme is insecure against the original signer's forgery. The security flaw of Park and Lee's original nominative proxy signature scheme is caused by the fact that the verifier does not use the public key of the proxy signer. To strengthen Park and Lee's scheme, Seo and Lee employed the public key of the proxy signer to prevent the original signer's forgery. However, Seo and Lee's scheme is still insecure against the original signer's forgery, that is, the original signer can generate a valid nominative proxy signature without the cooperation of the proxy signer. In the following, we will describe this attack.

Note that the original signer O knows the fact that the verifier V uses K_O in the signature verification. The original signer O chooses Y_P and computes $K'_O = Y_P^{-1} \bmod p$, $e' = h(W, T, K'_O)$, $S'_O = X_O e' \bmod q$, and $S'_P = S'_O \bmod q$. Next, O selects $r'_1, r'_2 \in_R Z_q^*$ and computes $K'_P = g^{r'_2 - r'_1} \bmod p$, $D' = Y_V^{r'_2} \bmod p$, $E' = h(Y_V, K'_P, D', M, W)$, $S' = r'_1 - S'_P E' \bmod q$, and sends $(M, Y_V, W, T, K'_O, K'_P, D', S')$ to V. Therefore, $(g^{S'}(Y_O^{e'}(Y_P K'_O)^{K'_O})^{E'} K'_P)^{X_V} = D' \bmod p$ holds and $(M, Y_V, W, T, K'_O, K'_P, D', S')$ is a valid nominative proxy signature. This is because:

$$(g^{S'}(Y_O^{e'}(Y_P K'_O)^{K'_O})^{E'} K'_P)^{X_V}$$
$$= (g^{r'_1 - S'_P E'}(g^{X_O e'}(Y_P Y_P^{-1})^{K'_O})^{E'} g^{r'_2 - r'_1})^{X_V} \bmod p$$
$$= (g^{r'_1 - S'_P E'} g^{S'_P E'} g^{r'_2 - r'_1})^{X_V} \bmod p$$
$$= (g^{r'_2})^{X_V} \bmod p$$
$$= D' \bmod p$$

To overcome this forgery attack, the improved nominative proxy signature scheme is given as follows: The original signer phase in the proposed scheme is the same as that of the Seo and Lee's scheme. The step 3 of the proxy signer phase is modified as follows.

Step 3: P selects $r_1, r_2, r_3 \in_R Z_q^*$ and computes $K_P = g^{r_2 - r_1} \bmod p$, $C_P = g^{r_3} \bmod p$, $Q_P = X_P K_O h(T, C_P) + r_3 \bmod q$, $D = Y_V^{r_2} \bmod p$, $E = h(Y_V, K_P, C_P, Q_P, D, M, W)$, and $S = r_1 - S_P E \bmod q$. Next, P sends the nominative proxy signature $(M, Y_V, W, T, K_O, C_P, Q_P, K_P, D, S)$ to V.

Next, the verifier phase is modified as mentioned below.

Step 1: V accepts K_O if $g^{Q_P} = Y_P^{K_O h(T, C_P)} C_P \bmod p$ holds, and then computes $e = h(W, T, K_O)$ and $E = h(Y_V, K_P, C_P, Q_P, D, M, W)$.

Step 2: V accepts $(M, Y_V, W, T, K_O, K_P, C_P, Q_P, D, S)$ as the nominative proxy signature if $(g^S(Y_O^e(Y_P K_O)^{K_O})^E K_P)^{X_V} = D \bmod p$ holds.

4 Discussions and Conclusion

According to the forgery attack in the previous section, we assume that the transmitted K_O in the original signer phase has been altered by the dishonest original signer O. That is, O modifies K_O with K'_O ($= Y_P^{-1} \bmod p$). Furthermore, O has to compute C'_P ($= g^{r'_3} \bmod p$) and Q'_P ($= X_P K'_O h(T, C'_P) + r'_3 \bmod q$) to convince V in the verifier phase, where Q'_P includes two unknown parameters. Obviously, O needs to know X_P and r_3 before computing Q'_P. However, this is computationally infeasible, because that O has to solve the discrete logarithm problem. An incorrect K_O can be detected in Step 1 of the verifier phase. That is, it is impossible for the original signer alone to alter K_O without the proxy signer's knowing. Therefore, the original signer's forgery attack cannot work in the proposed scheme.

The nominative proxy signature scheme should resist the original signer's forgery attack in which the original signer can cheat the honest verifier into believing a forged signature. We have shown that the modified nominative proxy signature scheme proposed by Seo and Lee still suffers from the original signer's forgery attack. In other words, the original signer can generate a valid nominative proxy signature without the proxy signer's help. The problem within Seo and Lee scheme is that the verifier cannot judge the correctness of K_O from the received signature. This paper further purposes an improvement to repair the security flaw.

Acknowledgements

This work was supported by the Brain Korea 21 Project of Kangwon National University in 2005.

References:

[1] M. Mambo, K. Usuda, and E. Okamoto, Proxy signature: delegation of the power to sign the message, IEICE Trans. Fundamentals, E79-A, 1996, pp. 1338–1353

[2] S. Kim, S. Park, and D. Won, Proxy signature, revisited, Proc. of ICICS '97, LNCS 1334, 1997, pp. 223–232

[3] K. Zhang, Threshold proxy signature schemes, Information Security Workshop, 1997, pp. 191–197

[4] B. Lee, H. Kim, and K., Kim, Strong proxy signature and its application, Proceedings of SCIS '2001, 2001, pp. 603–608

[5] K. Shum, and V. K. Wei, A strong proxy signature scheme with proxy signer privacy protection, Proceedings of the 11th IEEE

International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises 2002 (WETICE' 02), 2002, pp. 55–56

[6] H. U. Park, and I. Y. Lee, A digital nominative proxy signature scheme for mobile communication, Proc. of ICICS '2001, LNCS 2229, 2001, pp. 451–455

[7] S. H. Seo, and S. H. Lee, New nominative proxy signature scheme for mobile communication. Proceedings of SPI (Security and Protection of Information), 2003, pp. 149–154

[8] J. Li, Y. Zhang, and Y. Zhu, Security analysis and improvement of some proxy signature schemes, ACM Proceedings of the 3rd international conference on Information Security, 2004, pp. 27–32