2005 WSEAS Int. Conf. on DYNAMICAL SYSTEMS and CONTROL, Venice, Italy, November 2-4, 2005 (pp556-558)

Cryptanalysis of Li et al.'s Proxy Signature Scheme

KEON-JIK LEE* and BYEONG-JIK LEE
Dept. of Electrical&Computer Eng., Kangwon National University, Chuncheon, KOREA*
Dept. of Computer Eng., Kyungpook National University, Daegu, KOREA

Abstract: This work shows that the security improvement of Li *et al*. for Park and Lee's nominative proxy signature scheme is still insecure against the original signer's forgery. The problem within Li *et al*. scheme is that the verifier cannot judge the correctness of the parameter generated by the original signer from the received signature.

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

1 Introduction

A digital signature is a very important research area in cryptography. 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 [2–8]. 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. To construct a nominative proxy signature scheme, the following conditions must be satisfied.

- The original signer can delegate his signing capab ility to the proxy signer.
- Only the delegated proxy signer can nominate the verifier and create the nominative proxy signature.
- Only the nominee can verify the proxy signer's si gnature.
- If necessary, only the nominee can prove to the thi rd party that the signature was issued to him by th e nominator and it is valid.

Unfortunately, Sun and Hsieh [7] pointed out that Park and Lee's scheme is vulnerable to the original signer's forgery attack in which an original signer can cheat the honest verifier into believing a forged signature. Later, Li *et al*. [8] proposed a new scheme to enhance Park and Lee's scheme and claimed that their scheme can withstand the original signer's forgery attack. In this paper, we will review the scheme proposed by Li *et al*. and show that Li *et al*.'s scheme still suffers from the original signer's forgery attack.

2 Review of Li et al.'s scheme

Let p and q be large prime number with $q \mid (p-1)$, g be an element of order q in Z_p^*, $h(\ )$ be a secure one-way hash function, M be a message, T be a time stamp, W be a warrant which contains the identities of the original signer and proxy signer and valid period of delegation, etc, and X_U and Y_U ($= g^{XU} \bmod p$) be the private and public key of user U, respectively. The communicating entities O, P and V denote the original signer, the proxy signer and the verifier, respectively. We describe the scheme as follows and depict it as Fig. 1.

Original signer's phase:

O.1: O selects $r_0 \in_R Z_q^*$ and computes $K_O = g^{r_0} \bmod p$.
O.2: O computes $S_O = X_O Y_O h(M, W, T) + r_0 K_O \bmod q$ and then sends (M, W, T, K_O, S_O) to P.

Proxy signer's phase:

P.1: P accepts (M, W, T, K_O, S_O) if $g^{S_O} = Y_O^{Y_O h(M, W, T)} K_O^{K_O} \bmod p$ holds.
P.2: P computes the proxy signature key $S_P = S_O + X_P Y_P \bmod q$.
P.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 $(M, W, T, K_O, K_P, D, S)$ to V.

Verifier's phase:

V.1: V computes $E = h(Y_V, K_P, D, M, W)$.
V.2: V accepts $(M, W, T, K_O, K_P, D, S)$ as the nominative proxy signature if $(g^S (Y_O^{Y_O h(M, W, T)} K_O^{K_O} Y_P^{Y_P})^E K_P)^{X_V} = D \bmod p$ holds.

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

$$(g^S (Y_O^{Y_O h(M, W, T)} K_O^{K_O} Y_P^{Y_P})^E K_P)^{X_V} \bmod p$$
$$= (g^{r_1 - S_P E} (g^{X_O Y_O h(M, W, T) + r_0 K_O + X_P Y_P})^E g^{r_2 - r_1})^{X_V} \bmod p$$
$$= (g^{r_1 - S_P E} (g^{S_O + X_P Y_P})^E g^{r_2 - r_1})^{X_V} \bmod p$$
$$= (g^{r_1 - S_P E} (g^{S_P})^E g^{r_2 - r_1})^{X_V} \bmod p$$
$$= (g^{r_2})^{X_V} \bmod p$$
$$= D \bmod p$$

3 Cryptanalysis of Li *et al.*'s scheme

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, Li *et al*. employed the public key of the proxy signer to prevent the original signer's forgery. However, Li *et al.*'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 the novel attack.

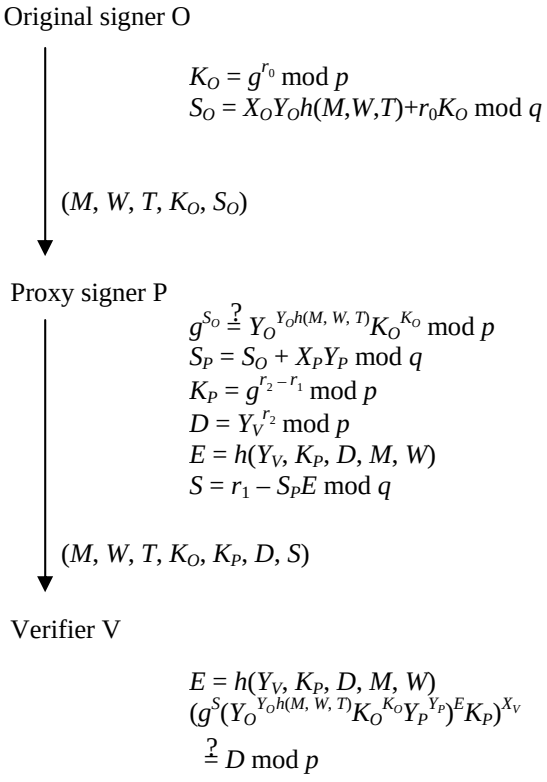

Fig. 1 Li *et al.*'s scheme

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 $K'_O = -Y_P \bmod p$, $S'_O = X_O Y_O h(M, W, T) \bmod q$, and $S'_P = S'_O \bmod q$. Next, O selects $r'_1, r'_2 \in_R Z_q^*$ and computes $K'_P = g^{r'_2 - r'_1} \bmod p$ (if Y_P is odd, $K'_P = -g^{r'_2 - r'_1} \bmod p$), $D' = Y_V^{r'_2} \bmod p$, $E' = h(Y_V, K'_P, D', M, W)$, $S' = r'_1 - S'_P E' \bmod q$, and sends $(M, W, T, K'_O, K'_P, D', S')$ to V. Therefore, $(g^{S'} (Y_O^{Y_O h(M, W, T)} K'^{K'_O}_O Y_P^{Y_P})^{E'} K'_P)^{X_V} = D' \bmod p$ holds and $(M, W, T, K'_O, K'_P, D', S')$ is a valid nominative proxy signature. This is because:

$$(g^{S'} (Y_O^{Y_O h(M, W, T)} K'^{K'_O}_O Y_P^{Y_P})^{E'} K'_P)^{X_V} \bmod p$$
$$= (g^{r'_1 - S'_P E'} (g^{X_O Y_O h(M, W, T)} (-Y_P)^{-Y_P} Y_P^{Y_P})^{E'} g^{r'_2 - r'_1})^{X_V} \bmod p$$
$$= (g^{r'_1 - S'_P E'} (g^{S'_P} (-1)^{-Y_P})^{E'} g^{r'_2 - r'_1})^{X_V} \bmod p$$

$= (g^{r'_2}(-1)^{-Y_P E'})^{X_V} \bmod p$

$= (g^{r'_2})^{X_V} \bmod p$

$= D' \bmod p$

4 Conclusion

We have shown that the enhanced nominative proxy signature scheme proposed by Li *et al*. still suffers from the original signer's forgery attack. We pointed out that the problem within Li *et al*. scheme is that the verifier cannot confirm the correctness of the parameter made by the original signer from the received proxy signature. This problem is the fundamental problem of Park and Lee's nominative proxy signature scheme.

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] H. M. Sun and B. T. Hsieh, On the security of some proxy signature schemes, Cryptology ePrint Archive. Report 2003/068

[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