Security Analysis of Lal and Awasthi's Proxy Signature Schemes

Manik Lal Das, Ashutosh Saxena and V P Gulati
Institute for Development and Research in Banking Technology,
Castle Hills, Road No.1, Masab Tank,
Hyderabad-500 057, INDIA.
Email:{mldas, asaxena, vpgulati}@idrbt.ac.in

Abstract

In this paper, we analyze two proxy signatures scheme [1], [2] proposed by Lal and Awasthi and found that both the schemes suffer with the security flaws. The scheme [1] suffers with proxy signer's forgery attacks and misuse of original signer's delegated information. The other scheme [2] suffers with original signer's forgery attack, proxy signer's undeniability and misuse of delegated information.
Keywords: proxy signature, delegation, warrant, forgery attacks.

1 Introduction

For a proxy signature, an original signer delegates his/her signing capability to a designated proxy signer and then the proxy signer performs the message signing on behalf of the original signer. Proxy signatures can be useful in numerous fields like distributed computing, electronic commerce, payment systems etc. Upon receiving a proxy signature, a verifier can validate its correctness by the signature verification procedure. The verifier can also check the original signer's agreement with the proxy signer from the received proxy signature since the proxy signature key is generated using the original signer's signature on delegated information. The following types of delegation are used for proxy signature schemes: Full Delegation, Partial Delegation and Delegation by Warrant.

-Full Delegation: An original signer directly gives his/her own secret key to a proxy signer. In this delegation, the distinguishability of proxy signature and original signature does not arise.

-Partial Delegation: An original signer does not give his/her own secret key, instead, derives a proxy key from it and passes to the proxy signer. The proxy signer generates a proxy signature on the message by using the proxy key, but with this proxy key, the proxy signer can abuse the original signer's delegated rights as it does not containg any warrant.

-Delegation by Warrant: The proxy signer is given by the original signer a proxy warrant that contains signers' identity information, delegation period, the qualification of the message on which the proxy signer can sign.

-Partial Delegation with Warrant: In partial delegation with warrant, a proxy key is computed from the original signer's secret key and a warrant. The proxy key is given to

the proxy signer, who can perform the signing operation on behalf of the original signer. A number of schemes and improvements have been proposed after the birth of Mambo et al scheme [3]. KPW [4] intorduced the concept of proxy signatures using partial delegation by warrant. Sun et al. [5] and Wang et al. [6] analyzed some proxy signature schemes which are insecure. Lal and Awasthi proposed two proxy signature schemes [1], [2], where [1] is for blind proxy signature scheme and [2] is for warrant recovery from the proxy signarure. In this paper, we show that Lal and Awasthi's proxy signature schemes [1], [2] are insecure.

Security Requirements: The basic security requirements of a proxy signatures scheme are unforgeability, nonrepudiaty, identifiability, verifiability and prevention of misuse, which are explined below.
SR1. Strong unforgeability: A proxy signer can create a valid proxy signature for the original signer. But the original signer and any third party cannot create a valid proxy signature with the name of a proxy signer.
SR2. Strong identifiability: Strong identifiability: Anyone can determine the identity of the corresponding proxy signer from a proxy signature.
SR3. Strong undeniability: Strong nonrepudiaty: Once a proxy signer creates a valid proxy signature for an original signer, he/she cannot repudiate his/her signature creation against anyone.
SR4. Verifiability: Any verifier can be convinced of the agreement of the original signer on the signed message from its corresponding proxy signature.
SR5. Prevention of misuse: The proxy signer is restricted to transfer the proxy key to someone else. If it does, the responsibility of the proxy signer is determined from the warrant.
The paper is organized as follows. Section 2 presents some notations and parameters used throughout the paper. In section 3, we review Lal and Awasthi's blind proxy signature scheme [1] and present the security flaws of their scheme. In section 4, we review Lal and Awasthi's proxy another scheme [2] and present the security flaws of their scheme. Finally, we conclude the work in section 5.

2 Notations and Parameters

Throughout this paper, we will use the following notations and parameters to explain and analyze the schemes.

p	A large prime (usually 1024 bits)
q	A prime factor of $p-1$ (usually 160 bits)
Z_p	Set of integers modulo p
Z_p^*	Multiplicative group of order q
g	Generator of order q in Z_p^*
k_o , k_p	Random Numbers $\in Z_q^*$
r_o , r_p	Transient public keys :r_o=g^{k_o}mod p and r_p=g^{k_p} mod p
x_o , x_p	The secret key of original and proxy signer respectively
y_o , y_p	Certified public key of original and proxy signer respectively where y_o=g^{x_o} mod p and y_p=g^{x_p} mod p
m_w	A warrant
$h(.)$	A collision-resistant cryptographic hash function

3 Review of Lal and Awasthi's Scheme [1] and Possible Attacks on the Scheme

The scheme [1] presents a proxy blind signature with which a proxy is able to make proxy blind signature and the verifier is able to verify the signature.

[Proxy Key Generation Phase]

(i) The original signer chooses random integer $k_o \in Z_q^*$ and computes $r_o = m_w g^{k_o} \bmod p$.

(ii) The original signer computes the proxy key $s = k_o\ r_o + x_o \bmod q$, and sends (s, r_o) to the proxy signer.

(iii) $y_p = g^s \bmod p$ is made public and the original signer sends $(y_p,\ r_o)$ to the proxy signer.

[Proxy Signature Generation Phase]

(i) The proxy signer verifies the proxy key s as $g^s = y_o (r_o)^{r_o} \bmod p$.

(ii) If it holds, the proxy signer chooses a random integer $k_p \in Z_q^*$, and computes $r_p = g^{k_p} \bmod p$, and sends r_p to receiver C.

(iii) A third person say, C chooses randomly $\alpha,\ \beta \in Z_q^*$, and computes $r = r_p g^{-\alpha} (g^s)^{-\beta} \bmod p$.

(iv) C computes $e = \beta + h(r \bigoplus m)$, and sends to proxy signer.

(v) The proxy signer computes $s' = k_p\text{-}s\ e \bmod q$, and sends it to C.

(vi) C computes $\sigma = s'\text{-}\alpha \bmod q$. The proxy blind signature of the message m is $(m,\ \sigma,\ h(r \bigoplus m))$.

[Signature Verification Phase]

(i) The verifier checks whether $h(r \bigoplus m) = h(g^{\sigma} (g^s)^{h(r \bigoplus m)} \bmod p \bigoplus \mathrm{m}) \bmod q$. If it holds, the signature $(m,\ \sigma,\ h(r \bigoplus m))$ is valid.

3.1 Attacks on the Scheme [1]

a. Proxy Signer's forgery Attack

(i) the proxy signer chooses a random integer $k_p \in Z_q^*$, and computes $r_p = g^{k_p} \bmod p$, and sends r_p to C.

(ii) C chooses randomly $\alpha,\ \beta \in Z_q^*$, and computes $r = r_p\ g^{-\alpha} (g^s)^{-\beta} \bmod p$.

(iii) C computes $e = \beta + h(r \bigoplus m)$, and sends to proxy signer.

(iv) The proxy signer chooses random integers $k, t \in Z_q^*$, and computes $R = g^k (y_p)^e t^{-1}$. We assume that $r_p = R.t$ exists. Then, the proxy signer sends k to C.

(v) C computes $\sigma = k$ - $\alpha \bmod q$. The proxy blind signature of the message m is $(m,\ \sigma,\ h(r \bigoplus m))$.

Correctness:

$h(g^{\sigma}(y_p)^{h(r \bigoplus m)} \bmod p \bigoplus m) \bmod q$

$=h(g^k g^{\alpha}(y_p)^{h(r \bigoplus m)} \bmod p \bigoplus m) \bmod q$

$=h(R\ t\ (y_p)^{-e} g^{-\alpha}(y_p)^{h(r \bigoplus m)} \bmod p \bigoplus m) \bmod q$

$=h(r_p(y_p)^{-\beta}(y_p)^{-h(r \bigoplus m)} g^{-\alpha}(y_p)^{h(r \bigoplus m)} \bmod p \bigoplus m) \bmod q$

$=h(r \bigoplus m) \bmod q$

b. Misuse of original signer's delegated information

As the original signer's delegation power does not contain any information about the qualification of the messages on which the proxy signer signs. The original signer cannot restrict the proxy signer for misuse of his/her delegation. The proxy signer can further transfer the delegation power to someone else, who also can perform the signing operation on behalf of the original signer.

4 Review of Lal and Awasthi's Scheme [2] and Possible Attacks on the Scheme

In this scheme, the authors present a digital proxy signature scheme in which the warrant message can be recovered from the proxy signature. We briefly review the scheme below.

[**Proxy Key Generation Phase**]

(i) The original signer chooses random integer $k_o \in Z_q^*$ and computes $r_o = m_w\ g^{k_o} \bmod p$.

(ii) The original signer computes the proxy key $s = k_o + r_o\ x_o \bmod q$, and sends (s, r_o) to the proxy signer.

[**Proxy Signature Generation Phase**]

(i) The proxy signer verifies the proxy key s as $m_w = g^{-s}(y_o)^{r_o}\ r_o \bmod p$.

(ii) If it holds, the proxy signer chooses random integer $k_p \in Z_q^*$, and computes $r_p = g^{k_p} \bmod p$.

(iii) The proxy signer computes the signature key $\sigma = s + k_p\ h(m, r_p) \bmod q$, and signs the message m.

(iv) The proxy signer sends the signature (m, σ, r_o, r_p) to the verifier.

[**Signature Verification Phase**]

(i) The verifier checks whether $m_w = g^{-\sigma}(y_o)^{r_o}\ r_o(r_p)^h(m, r_p) \bmod p$. If this holds, the signature is valid.

4.1 Attacks on the Scheme [2]

a. Original Signer's Forgery Attack

In the proxy signature generation phase, there is no use of secret key of the proxy signer. A dishonest original signer can impersonate his/her proxy signer by creating signature after giving delegation to the proxy signer.

b. Misuse of delegated information
Since the verification process does not contain any identity of the proxy signer, the responsibility of the proxy signer on the signed message is meaningless. The proxy signer can further delegate the proxy key to someone else, who can also perform the signing operation on behalf of the original signer.

c. Proxy Signer's Undeniability
As the verification phase does not include the proxy signer's key, the verifier cannot prove that the signed message has come from the proxy signer. The proxy signer can deny the signature made by him/her.

Moreover, the authors claimed that the warrant need not be hashed or sent along with the proxy signature and the verifier can recover the warrant during the verifiaction phase. We feel that their claim is not true as the transient key $r_o{=}m_w g^{k_o} \bmod p$ contains warrant and the entire scheme accompanied r_o.

5 Conclusions

In this paper, we briefly explained two proxy signature schemes proposed by Lal and Awasthi and showed that both the schemes are insecure as it does not satisfy forgeability, undeniability and prevention of misuse security requirements. Moreover, in the scheme [2] the authors claimed that proxy signature needs not to be accompanied by the warrant message, which is not true as the transient key $r_o{=}m_w g^{k_o} \bmod p$ contains warrant and the entire scheme accompanied r_o.

References

[1] S. Lal and A. Awasthi. Proxy Blind Signature Scheme. *IACR ePrint Archive, http://eprint.iacr.org/2003/72* , Report No.72 (2003).

[2] S. Lal and A. Awasthi. A Scheme for obtaining a Warrant Message from the Digital Proxy Signatures. *IACR ePrint Archive, http://eprint.iacr.org/2003/73* , Report No.73 (2003).

[3] M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures: Delegation of the power to sign messages. *IEICE Transactions Fundamentals* , E79-A, no.9, pp. 1338–1353,(1996).

[4] S. Kim, S. Park, and D. Won. Proxy Signatures Revisited. *ICICS'97, LNCS 1334* , pp. 223–232,(1997).

[5] H. Sun and B. Hsieh. On the Security of Some Proxy Signature Schemes. *IACR ePrint Archive, http://eprint.iacr.org/2003/68* , Report No.68 (2003).

[6] G. Wang, F. Bao, J. Zhou and R. Deng. Security Analysis of Some Proxy Signatures. *IACR ePrint Archive, http://eprint.iacr.org/2003/196* , Report No.196 (2003).