Further Cryptanalysis of some Proxy Signature Schemes

National Key Lab of Integrated Services Networks,
Xidian University, Xian, P.R.China
Jiqiang Lv, Jingwei Liu and Xinmei Wang
E-mail: lvjiqiang@sina.com

Abstract: Proxy signature is a signature that an original signer delegates his or her signing capability to a proxy signer, and then the proxy signer creates a signature on behalf of the original signer. However, H.Sun et al. showed that some exiting proxy signature are not against the original signer's forgery attack, so the schemes do not process the unforgeability property. In this paper, we present an extensive forgery method, which makes the forgery method of H.Sun et al. be a special case of ours.

Keywords: Public Key Cryptography; Proxy Digital Signature; Forgery Attack

1 Introduction

Proxy signature is a signature that an original signer delegates his or her signing capability to a proxy signer, and then the proxy signer creates a signature on behalf of the original signer. Mambo, et al. first gave a systematic discussion of proxy signatures and classified proxy signatures based on delegation type as full delegation, partial delegation and delegation by warrant[1]. Under the full delegation, the original signer gives his secret key to the proxy signer. Under the partial delegation, the original signer generates a proxy signature key by using his secret key and gives it to the proxy signer. The proxy signer uses the proxy key to sign. Accordingly, the verification equation for proxy signature is modified, so that the proxy signature is distinguishable from the signature signed by the original signer. Under the delegation by warrant, the proxy signer obtains the warrant which is a certificate composed of a message part and a public signature key from the original signer and uses the secret key to sign. The resulting signature consists of the created signature and the warrant. Later, B.Lee et al. provided new classifications of proxy signatures as strong vs. weak proxy signatures, designated vs. non-designated proxy signatures and self-proxy signatures[4]. Strong proxy signature represents both original signer's and proxy signer's signatures. Once a proxy signer creates a valid proxy signature, he cannot repudiate his signature creation against anyone. Weak proxy signature represents only original signer's signatures. It does not provide the non-repudiation of proxy signer. K.Shum et al. proposed a proxy signer-protected signature[7], during which, the real identity of a proxy signature is hidden to an alias. Only under the help of an authority could the real identity be revoked. However, H.Sun et al. showed that some exiting proxy signature are not against the original signer's forgery attack, so the schemes do not process the unforgeability property[8]. In this paper, we present an extensive forgery method, which makes the forgery method of H.Sun et al. be a special case of ours.

In the next section, we list some notations and domain parameters, and briefly describe some related proxy signature schemes in Section 3. In Section 4, we show our forgery method. A conclusion in the final section.

2 Notations and Domain Parameters

Throughout this paper, we will use the following notations and parameters,

p : a public large prime

q : a public large prime factor of $p-1$

g : a public base element of order q in Z_p

$h(\cdot)$: a public one-way hush function

x_o : original signer's secret key

y_o : original signer's corresponding public key, where $y_o = g^{x_o} \bmod p$

x_p : proxy signer's secret key

y_p : proxy signer's corresponding public key, where $y_p = g^{x_p} \bmod p$

m_w : a warrant

3 Some Related Proxy Signature Schemes

In this section, we briefly descript the proxy and multi-proxy signature schemes of B.Lee et al. and the proxy signature scheme of K.Shum et al.

3.1 Proxy Signature Scheme of B.Lee et al.

Proxy key generation

The original signer *O* selects $k_0 \in_R Z_q^\bullet$, and computes $r_0 = g^{k_0} \bmod p$ and $s_0 = x_0 \cdot h(m_w, r_0) + k_0 \bmod q$. Then he sends (m_w, r_0, s_0) to the proxy signer P.

P accepts (m_w, r_0, s_0) as a valid proxy key from *O* if $g^{s_0} = y_0^{h(m_w, r_0)} r_0 \bmod p$ holds.

Proxy signature generation

P computes the proxy signature key $x_{pr} = s_0 + x_p \bmod q$, and generates the proxy signature s of a message *m* by using the proxy signature key. Then, P sends (m, s, m_w, r_0) to the verifier V.

Signature Verification

V computes the proxy public key $y_{pr} = y_0^{h(m_w, r_0)} r_0 \cdot y_p \bmod p$, and then verifies the signature s by using the DLP-like signature scheme.

3.2 Multi-Proxy Signature Scheme of B.Lee et al.

Let *O_i* be the group of *n* original signers, (x_i, y_i) be their corresponding secret and public key pairs.

Multi-Proxy key generation

The original signer O_i selects $k_i \in_R Z_q^\bullet$, and computes $r_i = g^{k_i} \bmod p$ and $s_i = x_i \cdot h(m_{w_i}, r_i) + k_i \bmod q$. Then he sends (m_{w_i}, r_i, s_i) to the proxy signer P.

P accepts (m_{w_i}, r_i, s_i) as a valid proxy key from O_i if $g^{s_i} = y_i^{h(m_{w_i}, r_i)} r_i \bmod p$ holds.

Proxy signature generation

P computes the proxy signature key $x_{pr} = \sum_{i=1}^{n} s_i + x_p \bmod q$, and generates the proxy signature s of a message m by using the proxy signature key. Then, P sends $(m, s, m_{w_1}, r_1, \cdots, m_{w_n}, r_n)$ to the verifier V.

Signature Verification

V computes the proxy public key $y_{pr} = \prod_{i=1}^{n} \left(y_i^{h(m_{w_i}, r_i)} r_i \right) \cdot y_p \bmod p$, and then verifies the signature s by using the DLP-like signature scheme.

3.3 Proxy Signature Scheme of K.Shum et al.

Alias issuing

P sends his identity ID_p to T.

T selects $k_p \in_R Z_q^{\bullet}$ and $k_T \in_R Z_q^{\bullet}$, computes $h_p = h(k_p, ID_p)$, $r_T = g^{k_T} \bmod p$ and $s_T = x_T \cdot h(h_p, r_T) + k_T \bmod q$. Then he sends (h_p, r_T, s_T) to P.

P accepts the triplet (h_p, r_T, s_T) if $g^{s_T} = y_T^{h(h_p, r_T)} r_T \bmod p$ holds.

Proxy key generation

The original signer O selects $k_0 \in_R Z_q^{\bullet}$, and computes $r_0 = g^{k_0} \bmod p$ and $s_0 = x_0 \cdot h(m_w, r_0) + k_0 \bmod q$. Then he sends (m_w, r_0, s_0) to the proxy signer P.

P accepts (m_w, r_0, s_0) as a valid proxy key from O if $g^{s_0} = y_0^{h(m_w, r_0)} r_0 \bmod p$ holds.

Proxy signature generation

P computes the proxy signature key $x_{pr} = s_0 + s_T \bmod q$, and generates the proxy signature s of a message m by using the proxy signature key. Then, P sends

$(m, s, m_w, r_0, h_p, r_T)$ to the verifier V.

Signature Verification

V computes the proxy public key $g^{x_{pr}} = y_0^{h(m_w, r_0)} r_0 \cdot y_T^{h(h_p, r_T)} r_T \mod p$, and then verifies the signature s by using the DLP-like signature scheme.

Privacy revoking

V sends the alias h_p to T. Next, T returns k_p and ID_p to V. V accepts that the signer's identity is ID_p if $h_p = h(k_p, ID_p)$ holds.

4 Our Attacks

4.1 Attack on the Proxy Signature Scheme of B.Lee et al.

A dishonest original signer O randomly selects $a, b \in_R Z_q^{\bullet}$, and computes

$$\tilde{r}_0 = y_p^{-1} y_0^a g^b \mod p,$$

$$\tilde{x}_{pr} = x_0 \cdot \left(h(m_w, \tilde{r}_0) + a \right) + b \mod q.$$

Now, $\tilde{x}_{pr}$ is an illegal secret key of his proxy signer.

4.2 Attack on the Multi-Proxy Signature Scheme of B.Lee et al.

A dishonest original signer O_j randomly selects $a, b \in_R Z_q^{\bullet}$, and computes

$$\tilde{r}_j = y_p^{-1} y_j^a g^b \mod p \quad,$$

$$\tilde{x}_{pr} = x_j \cdot \left(h(m_{w_j}, \tilde{r}_j) + a \right) + b \mod q$$

Now, $\tilde{x}_{pr}$ is an illegal secret key of his proxy signer.

4.3 Attack on the Proxy Signature Scheme of K.Shum et al.

A dishonest original signer O randomly selects $a, b \in_R Z_q^{\bullet}$, and computes

$$\tilde{r}_0 = y_p^{-1} y_0^a g^b \bmod p \,,$$

$$\tilde{x}_{pr} = x_0 \cdot \left(h(m_w, \tilde{r}_0) + a \right) + b \bmod q$$

Now, $\tilde{x}_{pr}$ is an illegal secret key of his proxy signer.

Notice that a dishonest T can also impersonate his user in the same way. Furthermore, we should point out that the proxy signature scheme of K.Shum et al. is unpratical, for a verifier can determine by himself whether a signature comes from a person which is exposed to him by T before.

5 Conclusion

we further cryptanalyze some proxy signature schemes, and present an extensive forgery method, during which a dishonest original signer can impersonate his proxy signers, so the related proxy signature schemes is insecure.

Acknowledgement:
This work was supported by China National 973 Project Found(G1999035804)

References

1. M.Mambo, K.Usuda and E.Okamoto: Proxy Signature:Delegation of the Power to Sign Messages, *IEICE Trans.Fundamentals*,Vol.E79-A:No.9,pages 1338-1353, 1996.
2. T.ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on Information Security*,IT-31, pp.469-472,1985.
3. S.Kim, S.Park and D.Won: Proxy Signatures, revisited, *Proc. of ICICS'97-First International Conference on Information and Communication Security*. Springer-Verlag, LNCS 1334,pp.223-232, 1997.
4. B.Lee, H.Kim and K.Kim, Strong Proxy Signature and its Applications, *Proc. of SCIS-Sypsium on Cryptology and Information Security*, pp.603-608,2001.
5. B.Lee, H.Kim and K.Kim, Secure Mobile Agent Using Strong Non-designated Proxy Signature, *Proc. of ACISP2001*, Springer-Verlag, LNCS 2119, pp.474-486, 2001.
6. K.Zhang: Threshold Proxy Signature Schemes, *Proc.of 1st International Information Security Worshop*, pp. 282-290,1997.
7. K.Shum and V.Wei, A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection. *Proc. of WETICE'02-Eleventh IEEE International Collaborative*

Enterprises,pp.55-56,2002.

8. H.Sun and B.Hsieh, On the Security of some Proxy Signature Schemes. Available at *http://eprint.iacr.org/2003/068*