Cryptanalysis of Park-Lee Nominative Proxy Signature Scheme

Zhengjun Cao

Institute of Systems Science, Academy of Mathematics and Systems Science,

Chinese Academy of Sciences, Beijing, P.R. China. 100080 (zjcamss@hotmail.com)

Abstract Park and Lee have proposed a digital nominative proxy signature scheme for mobile communication in [1]. They claimed that neither Origin signer nor Proxy agent can generate a valid signature solely. In this paper we show that Origin signer can generate a valid signature without the cooperation of the agent. In fact, the flaw comes from that Verifier dose not use the public key of Proxy agent in verifying phase. It's a serious designing error.

Keywords Proxy signature.

1 Introduction

Based in the development of mobile communication, the future mobile communication systems are expected to provide higher quality of multimedia services for users than current systems. Therefore, many technical factors are needed in these systems. Especially the secrecy and safety would be acquired through the introduction of the security for mobile communication. So in paper [1], the authors proposed a digital nominative proxy signature scheme for mobile communication. They claimed that:

> Providing safety: When a signature request information is sent to proxy agent, <u>a origin</u> gives one time secret signature information. Also when the signature is generated by proxy agent, he input his secret information to the signature. Because <u>a origin</u> and proxy agent <u>dose not</u> can generate <u>a illegal</u> signature, this scheme provides the safety.

Actually, the scheme should satisfy the following property: Neither Origin signer nor Proxy agent can generate a valid proxy signature solely.

In this paper we show that Origin signer can generate a valid signature without the cooperation of the agent. In fact, the flaw comes from that Verifier dose not use the public key of Proxy agent in verifying phase. It's a serious designing error.

The paper is organized as follows: Section 2 reviews the proxy signature. In section 3, we present an attack to show that Origin signer can generate a valid proxy signature solely. Some conclusion remarks will be presented in section 4.

2 Review of the nominative proxy signature scheme

2.1 System Parameter

p, q: a large prime number $p \geq 512$ bit, $q|p-1$

g: $\in Z_p^*$ of order q (Not: g is a generator for Z_p^*, see [1])

X_A, X_B, X_G: Origin signer A, Verifier B and Proxy agent's secret information

$Y_A \equiv g^{X_A}$ $modp$: A's common information

$Y_B \equiv g^{X_B}$ $modp$: B's common information

$Y_G \equiv g^{X_G}$ $modp$: Proxy agent's common information

s_i: Origin signer's one-time secret information for a signature($i \in_R Z$)

T_i, M: i'th time-stamp and message

$H()$: secure 128bit one-way hash function

2.2 Implementing Nominative Proxy Signature

2.2.1 Proxy generation

Origin signer A generates a signature request information as follows:

$$\begin{aligned}
&a_i \in_R Z_q^* \quad (\underline{\text{Not: } a_i \in_R Z^p(i \in_R Z), see[1]})\\
&d_i \equiv H(M \parallel T_i)\\
&l \equiv g^{a_i} \ mod\ p\\
&s_i \equiv (X_A \cdot d_i + a_i \cdot l) \ mod\ q \ \underline{\text{(Not: mod } p\text{, see [1])}}
\end{aligned}$$

Origin signer A gives (s_i, l, M, T_i) to the proxy agent, G, in a secure manner.

2.2.2 Proxy verification

G checks

$$g^{s_i} \stackrel{?}{\equiv} (Y_A^{H(M \| T_i)} l^l) \ \ mod\ p$$

If it does not hold, G rejects.

2.2.3 Nominative proxy signing

G chooses two random number $r, R \in Z_p^*$, computes:

$$\begin{aligned} K &\equiv g^{R - rX_G} \quad \bmod \ p \\ D &\equiv Y_B^R \quad \bmod \ p \\ e &\equiv H(Y_B \parallel K \parallel D \parallel M) \\ S_a &\equiv (X_G \cdot r - R \cdot s_i \cdot e) \ mod \ p \end{aligned}$$

Proxy agent G sends $(M, T_i, l, K, D, R, S_a)$ to Verifier B.

2.2.4 Verification of the nominative proxy signature

Verifier B computes:

$$\begin{aligned} e &\equiv H(Y_B \parallel K \parallel D \parallel M) \\ b &\equiv (Y_A^{H(M \| T_i)} \cdot l^l) \ mod \ p \end{aligned}$$

Check

$$(g^{s_a} b^{R \cdot e} K)^{X_B} \stackrel{?}{\equiv} D \ \ mod \ p$$

If it holds, then B accepts the proxy signature.

Correctness:

$$\begin{aligned} (g^{s_a} b^{R \cdot e} K)^{X_B} &\equiv (g^{r \cdot X_G - R \cdot s_i \cdot e} (Y_A^{H(M \| T_i)} \cdot l^l)^{R \cdot e} g^{R - r \cdot X_G})^{X_B} \\ &\equiv (g^{r \cdot X_G - R \cdot s_i \cdot e} (g^{a_i \cdot l + X_A \cdot H(M \| T_i)})^{R \cdot e} g^{R - r \cdot X_G})^{X_B} \\ &\equiv (g^R)^{X_B} \equiv (Y_B)^R \equiv D \ \ (mod \ p) \end{aligned}$$

3 Analysis

In this section, we should point out that the scheme have many flaws not only in description of protocol (such as above underlined parts) but in processing data. In fact, Verifier B does not use the Proxy agent G's public information Y_G to check the validity of received proxy signatures. Obviously, it's easy for Origin signer A to forge a valid proxy signature solely.

Now we introduce an attack on the scheme as follows: For a given message M, and time-stamp T_i, Origin signer A only needs to choose three random numbers $\alpha, \beta, R \in Z_p^*$, computes:

$$l \equiv g^\alpha, \quad K \equiv g^\beta, \quad D \equiv Y_B^R \quad (mod \ p)$$

$$S_a \equiv R - \beta - R \cdot H(Y_B \parallel K \parallel D \parallel M) \cdot [x_A \cdot H(M \parallel T_i) + \alpha g^\alpha] \ \ mod \ q$$

Then he sends $(M, T_i, l, K, D, R, S_a)$ to Verifier B.

Correctness:

$$\begin{aligned} e &\equiv H(Y_B \parallel K \parallel D \parallel M) \\ b &\equiv (Y_A^{H(M\|T_i)} \cdot l^l) \ mod\ p \\ (g^{s_a} b^{R \cdot e} K)^{X_B} &\equiv (g^{S_a} (Y_A^{H(M\|T_i)} \cdot l^l)^{R \cdot e} g^{\beta})^{X_B} \\ &\equiv (g^{S_a + \beta + R \cdot H(Y_B \| K \| D \| M) \cdot [x_A \cdot H(M \| T_i) + \alpha g^{\alpha}]})^{X_B} \\ &\equiv (g^R)^{X_B} \equiv (Y_B)^R \equiv D \quad (mod\ p) \end{aligned}$$

4 Conclusion

In this paper, we presented a simple and direct attack on Park-Lee nominative proxy signature scheme. Our results show that the scheme is very fragile.

References

[1] Hee-Un Park and Im-Yeong Lee, A digital nominative proxy signature scheme for mobile communication, ICICS 2001, LNCS 2229, PP. 451-455, 2001. Springer-Verlag.