Attacks on a threshold proxy signature scheme based on the RSA cryptosystem

YUH-DAUH LYUU
Dept. of Computer Science & Information Engineering and Dept. of Finance
National Taiwan University
No 1, Sec 4, Roosevelt Rd, Taipei, Taiwan

MING-LUEN WU
Dept. of Computer Science & Information Engineering
National Taiwan University
No 1, Sec 4, Roosevelt Rd, Taipei, Taiwan
and
Dept. of Information Management
Chung-Yu Institute of Technology
No. 40, Yi-7th Rd, Keelung, Taiwan

Abstract: - Recently, Hwang et al. propose an efficient (t, n) threshold proxy signature scheme in which the original signer can authorize n proxy signers such that only the cooperation of t or more of them is able to generate a proxy signature on behalf of the original signer. Their scheme is based on the RSA cryptosystem. They claim that any t out of n proxy signers cannot derive the original signer's private key. This paper disproves this claim by showing that their system can be broken using only the public information. This result is obtained without even the need to obtain ciphertext or the factorization of the RSA modulus. Hence the signature scheme of Hwang et al. is insecure.

Key-Words: - Cryptography, Threshold proxy signature, RSA, Lagrange interpolation, Cryptanalysis.

1 Introduction

A (t, n) threshold proxy signature scheme allows the original signer to authorize n proxy signers such that only the cooperation of t or more proxy signers is able to generate a proxy signature on behalf of him [2–4, 6–8]. In 2003, Hwang et al. present an efficient threshold proxy signature scheme based on the RSA cryptosystem [3, 5]. Their scheme is divided into three phases: proxy sharing, proxy signature issuing, and verification. In the proxy sharing phase, the original signer computes the partial proxy signing keys from his private key and sends them to each authorized proxy signer. In the proxy signature issuing phase, t proxy signers with their proxy signing keys cooperate to generate a proxy signature on a message. In the verification phase, proxy signatures are verified and the actual proxy signers can be identified.

In Hwang et al.'s scheme, each signer has his own public and private keys as in the RSA cryptosystem. They claim that even the cooperation of any t proxy signers cannot obtain the original signer's private key. Their argument is essentially based on the difficulty of the factorization of the RSA modulus. This paper disproves this claim by showing that their system can be easily broken using only the public information. This result is obtained without even the need to obtain ciphertext or the factorization of the RSA modulus. Hence the signature scheme of Hwang et al. is insecure.

2 The proxy sharing phase of Hwang et al.'s scheme

In Hwang et al.'s scheme, there are three types of players. They are original signer P_0, proxy signers $P_1, P_2, \ldots, P_n$, and the combiner. The combiner manages to generate proxy signatures with the help of proxy signers. The scheme has three phases: proxy sharing, proxy signature issuing, and verification. Each signer uses the RSA cryptosystem [5]. Let P_i's public key be (e_i, N_i) and private key be d_i, $i = 0, 1, \ldots, n$. Note that modulus N_i is the product of two large primes p_i and q_i such that $e_i d_i \equiv 1 \pmod{\phi(N_i)}$ and $\gcd(e_i, \phi(N_i)) = 1$, where $\phi(N_i) = (p_i - 1)(q_i - 1)$. $m^{d_i} \bmod N_i$ is m signed with P_i's private key, and $m^{e_i} \bmod N_i$ is m encrypted with P_i's public key, using the RSA cryptosystem. In addition, let w denote the warrant that contains important information such as the expiration time of the proxy key, and the identities of the original signer and proxy signers. Denote by $||$ the concatenation of two strings. P_i's identity will be the number i.

Because Hwang et al.'s scheme can be broken right after the proxy sharing phase, we describe this phase in the following.

1. (Proxy generation). P_0 generates the proxy signature key D and its corresponding proxy verification key E, where

   $$\begin{aligned} D &= d_0^w \bmod \phi(N_0), \\ E &= e_0^w \bmod \phi(N_0). \end{aligned}$$

   P_0 publishes $(w, E, (w||E)^{d_0} \bmod N_0)$.

2. (Proxy sharing). P_0 randomly generates a secret polynomial f of degree $t-1$,

   $$f(X) = D + a_1 X + \cdots + a_{t-1} X^{t-1} \bmod \phi(N_0),$$

   where $a_1, a_2, \ldots, a_{t-1}$ are random integers modulo $\phi(N_0)$. P_0 computes P_i's partial proxy signing key $k_i = f(i)$ and sends $(k_i^{d_0} \bmod N_0 || k_i)^{e_i} \bmod N_i$ to P_i.

3. (Proxy sharing generation). After receiving $(k_i^{d_0} \bmod N_0 || k_i)^{e_i} \bmod N_i$, each P_i can decrypt it to obtain $k_i^{d_0} \bmod N_0$ and k_i. Each P_i then confirms the validity of k_i and keeps it secret.

Let T be a set of t numbers. Polynomial $f(X)$ can be expressed as a Lagrange interpolating polynomial [1],

$$f(X) = \sum_{i \in T} L_i(X) f(i) \bmod \phi(N_0),$$

where

$$L_i(X) = \prod_{i,j \in T, j \neq i} \frac{X - j}{i - j}.$$

Now,

$$\begin{aligned} D &\equiv f(0) \\ &\equiv \sum_{i \in T} L_i(0) f(i) \pmod{\phi(N_0)}. \end{aligned} \tag{1}$$

3 The attack

We will show that using only the public information, anyone can obtain $d \in \mathbb{Z}$ such that $e_0 d \equiv 1 \pmod{\phi(N_0)}$. As this d and the actual d_0 differ by some integer multiple of $\phi(N_0)$, it will work exactly as d_0, thus breaking the original signer's cryptosystem. This result is obtained without even the need to obtain ciphertext or the factorization of N_0. Our attack algorithm is described as follows.

Input: The public parameters e_0, N_0, w, E.

Output: An integer d such that $e_0 d \equiv 1 \pmod{\phi(N_0)}$.

Step 1: Compute $e_0^w - E$.

Step 2: Compute g according as

$$g = \gcd(e_0^{\lceil \log_2(e_0^w - E) \rceil}, e_0^w - E).$$

Step 3: Compute

$$N = \frac{e_0^w - E}{g}.$$

Step 4: Solve for d satisfying $e_0 d \equiv 1 \pmod{N}$.

Step 5: Output d.

Now we prove that $e_0 d \equiv 1 \pmod{\phi(N_0)}$.

Proof. As $e_0^w \equiv E \pmod{\phi(N_0)}$, we can write $e_0^w - E = r\phi(N_0)$ for some integer r. Note that the attacker does not know r. As $\gcd(e_0, \phi(N_0)) = 1$, we have $\gcd(e_0^{\lceil \log_2(e_0^w - E) \rceil}, r) = g$. So $N = \frac{e_0^w - E}{g} = r'\phi(N_0)$, where $r' = r/g$ is an integer. Clearly $\gcd(e_0, N) = 1$. Thus a d satisfying $e_0 d \equiv 1 \pmod{N}$ exists and is unique modulo N. Hence we have $e_0 d \equiv 1 \pmod{\phi(N_0)}$ because $\phi(N_0) | N$. □

From the above proof, we know that any integer multiple of $\phi(N_0)$ can be used to replace $e_0^w - E$ in the attack algorithm. Next we show how any t proxy signers can derive a smaller integer that is an integer multiple of $\phi(N_0)$. Assume that T is the set of the t proxy signers' identities. They compute D' as

$$D' = \sum_{i \in T} L_i(0) k_i.$$

Note that in Hwang et at.'s scheme, all $L_i(0)$ must be integers. By Eq. (1), we have $D' \equiv D \pmod{\phi(N_0)}$ because $k_i = f(i)$. So

$$\begin{aligned} D'E &\equiv DE \\ &\equiv d_0^w e_0^w \\ &\equiv 1 \pmod{\phi(N_0)}. \end{aligned}$$

Hence $\phi(N_0) | (D'E - 1)$.

4 Conclusions

In this paper, we have shown that Hwang et al.'s scheme can be broken with only the public information. This result is obtained without even the the need to obtain ciphertext or the factorization of the RSA modulus. If any t or more proxy signers collude, the attack can be made even more efficient. Hwang et al.'s scheme is therefore insecure.

References:

[1] R. L. Burden and J. D. Faires, *Numerical Analysis.* PWS Publishers, 4th ed., 1988.

[2] C.-L. Hsu, T.-S. Wu, and T.-C. Wu, "New repudiable threshold signature scheme with known signers," *The Journal of Systems and Software*, vol. 58, pp. 119–124, 2001.

[3] M.-S. Hwang, E. J.-L. Lu, and L.-C. Lin, "A practical $(t,,n)$ threshold proxy signature scheme based on the RSA cryptosystem," *IEEE Transactions on Knowledge and*

Data Engineering, vol. 15, no. 6, pp. 1552–1560, 2003.

[4] S. Kim, S. Park, and D. Won, “Proxy signatures, revisited,” in *Information and Communications Security—ICICS’97*, vol. 1334 of *LNCS*, pp. 223–232, Springer-Verlag, 1997.

[5] R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *CACM*, vol. 21, pp. 120–126, Feb. 1978.

[6] H.-M. Sun, “An efficient nonrepudiable threshold proxy signature scheme with known signers,” *Computer Communications*, vol. 22, pp. 717–722, 1999.

[7] C.-S. Tsai, S.-F. Tseng, and M.-S. Hwang, “Improved non-repudiable threshold proxy signature scheme with known signers,” *INFORMATICA: An International Journal*, vol. 14, no. 3, pp. 393–402, 2003.

[8] K. Zhang, “Threshold proxy signature schemes,” in *Information Security, First International Workshop, ISW ’97*, vol. 1396 of *LNCS*, pp. 282–290, Springer-Verlag, 1998.