Cryptanalysis of a Threshold Proxy Signature Scheme*

Hung-Min Sun(孫宏民), Cheng-Ta Yang(楊政達)†, Bin-Tsan Hsieh(謝濱燦)†
Department of Computer Science, National Tsing-Hua University
E-mail: hmsun@cs.nthu.edu.tw

†Department of Computer Science and Information Engineering
National Cheng Kung University

Abstract

A (t, n) threshold proxy signature scheme allows t or more proxy signers out of a designated group of n proxy signers to sign messages on behalf of an original signer. Recently, Hwang et al. proposed a new (t, n) threshold proxy signature scheme based on the RSA cryptosystem. In this paper, we show that their scheme is insecure against the original signer's forgery and the general forgery.

Keywords: Proxy Signatures, Digital Signatures, Cryptanalysis, Cryptography, RSA.

1 Introduction

Digital signature scheme [1][2][4][5] is an important research topic in cryptography. An ordinary digital signature scheme allows a signer to create signatures of documents and the generated signatures can be verified by any person. A digital signature scheme provides authenticity and non-repudiation of the signed message which are important properties required in e-commerce. A proxy signature scheme [6][7], a variation of ordinary digital signature scheme, enables a proxy signer to sign messages on behalf of the original signer. Proxy signature schemes have been shown to be useful in many applications. For example, a manager can delegate his secretaries to sign documents while he is on vacation. In general, there are three different types of delegation: full delegation, partial delegation, and delegation by warrant. In full delegation, the original signer gives his secret key to the proxy signer directly. The proxy signer uses the key to create signatures of documents which are the same as those created by the original signer. Therefore, full delegation is not practical because proxy signatures issued by the original signer and by the proxy signer are indistinguishable. In partial delegation, the proxy signature signing key is

*This research was supported by the Communications Software Technology project of Institute for Information Industry and sponsored by MOEA ,R.O.C.

generated by the proxy signer with the help of the original signer. Only the proxy signer can know the proxy signature signing key which can be used to generate valid proxy signatures; even the original signer can not. However, this approach suffers from the disadvantage that the proxy signature signing key is transferable. In delegation by warrant, the original signer signs a warrant which describes the relative rights and information of the original signer and proxy signer such that a signature verifier can use the warrant as a part of verification information. Usually, delegation by warrant incurs more computational cost than the other two. In [8], Kim *et al.* proposed a proxy signature scheme which is a partial delegation with warrant enjoying the computational advantage over the proxy signature by warrant and the structure advantage over the proxy signature for partial delegation. Since then, several variant schemes of proxy signature have been proposed to achieve the varied specific requirements in a proxy signature situation, e.g., threshold proxy signature[9][10], convertible proxy signature[11], time-stamped proxy signatures[12], proxy multi-signature[13],...., etc. Among them, a (t, n) threshold proxy signature scheme is a scheme which allows any t or more proxy signers from a designated group of n proxy signers to cooperatively sign messages on behalf of the original signer, while t-1 or less proxy signers cannot generate any valid proxy signatures. A (t, n) threshold proxy signature scheme should provide good security properties as follows:

- Proxy Protected Property: Only designated proxy signers can generate their partial proxy signatures respectively. Even the original signer can not masquerade as any proxy signer to generate a legal partial proxy signature, which is for generating a legal proxy signature by combining t legal partial proxy signatures. This also includes that the original signer can not forge a legal proxy signature directly, and then claim that the proxy group generates the proxy signature. This property is for protecting the authority of the proxy signers and the proxy group.

- Unforgeability Property: Only any t or more proxy signers from a designated group of n proxy signers can create a valid proxy signature on behalf of the original signer. Even the original signer can not generate a valid proxy signature due to the above proxy protected property. Any t-1 or less proxy signers cannot generate a legal proxy signature, either.

- Nonrepudiation Property: The proxy group and the corresponding proxy signers can not repudiate the valid proxy signatures that they have ever created This is due to the above unforgeability property.

Recently, Hwang et al. [3]proposed a new (t, n) threshold proxy signature scheme based on the RSA cryptosystem using a simple Lagrange formula to share the proxy signing key. They claimed that their (t, n) threshold proxy signature scheme satisfies all proxy signature requirements. In this paper, we show that Hwang et al.'s threshold proxy signature scheme is insecure against the original signer's forgery. Furthermore, we point out that their scheme is also insecure against a general forgery attack in which the proxy signer can not exactly confirm the validity of the partial proxy signing key, and the combiner can not exactly confirm the validity of the partial proxy signature.

2 Review Hwang et al.'s Threshold Proxy Signature Scheme

Hwang et al.'s threshold proxy signature scheme is based on the RSA cryptosystem. There are three phases: the proxy sharing phase, the proxy signature issuing phase, and the verification phase in their scheme.

Throughout this correspondence, we use P_0 to denote the original signer and P_1,P_2,...,P_n to denote the proxy signers. N_i is a public RSA modulus for every proxy signer P_i such that $N_i = p_i \times q_i$, where p_i and q_i are two large primes. Every proxy signer P_i has a private key d_i and a corresponding public key e_i, such that $d_i \times e_i = 1 \bmod \phi(N_i)$, where $\phi(N_i) = (p_i - 1)(q_i - 1)$ is the Euler totient function of N_i. The parameter e_i and N_i are published as the proxy signer P_i''s public key, and the parameter d_i and $\phi(N_i)$ are kept secret by the proxy signer P_i'. In their scheme, there are three roles: the original signer, the n proxy signers, and a combiner. In addition, the original signer constructs a warrant m_w that contains some important information including the validity period of the proxy key, the identities of the proxy signers and the original signer,etc.

We briefly review the Hwang et al.'s scheme as follows:

2.1 The proxy sharing phase

In the proxy sharing phase, the original signer P_0 delegates his signing power to n proxy signers during a stipulated period. The original signer generates the proxy key according to the following steps:

1. Proxy generation: The original signer P_0 generates a pair of group proxy key (D, E), where D is a group proxy signature key and E is a proxy verification key satisfying $D = d_0^{m_w} \bmod \phi(N_0)$,and $E = e_0^{m_w} \bmod \phi(N_0)$. Then, P_0 publishes $\{m_w, E, (m_w||E)^{d_0} \bmod N_0\}$.

2. Proxy sharing: The original signer P_0 randomly chooses $a_1, a_2, ..., a_{t-1}$ to generate a secret polynomial f of degree $t - 1$, as

$$f(x) = D + \sum_{i=1}^{t-1} a_i x^i \bmod \phi(N_0),$$

   and computes the proxy signers' partial proxy signing key, $k_i = f(i)$. Then he securely sends his signature on k_i, that is $({k_i}^{d_0} \bmod N_0||k_i)^{e_i} \bmod N_i$, to the proxy signer P_i, where i is the proxy signer's identity.

3. Proxy share generation: Each proxy signer P_i decrypts $({k_i}^{d_0} \bmod N_0||k_i)^{e_i} \bmod N_i$ with his decryption key d_i, and hence obtains $\{{k_i}^{d_0} \bmod N_0, k_i\}$. Then each proxy signer P_i confirms the validity of the partial proxy signing key k_i by checking whether the original signer's signature verification equation: $({k_i}^{d_0} \bmod N_0)^{e_0} \bmod N_0 = k_i$ holds or not. If it holds, the proxy signer P_i believes that k_i is correct and valid.

2.2 The proxy signature issuing phase

In the designated group, the group T of any t proxy signers want to sign a message M on behalf of the original sign cooperatively. The proxy signature issuing steps are in the following.

Each actual proxy signer P_i in group T signs M with his partial proxy signing key k_i in order to obtain his partial proxy signature s_i as follows:

$$s_i = M^{(L_i \times k_i)} \bmod N_0, \text{where } L_i = \prod_{i,j \in T, j \neq i} \frac{-j}{i-j}.$$

And then, each actual proxy signer sends $\{{s_i}^{d_i} \bmod N_i, s_i\}$ to the combiner. After receiving and verifying the partial proxy signature s_i using the proxy signer's public key e_i, the combiner generates the proxy signature S on the message M as

$$S = \prod_{i \in T} s_i \bmod N_0 (= M^D \bmod N_0).$$

2.3 The verification phase

The receiver can obtain and confirm the proxy verification key E by using the original signer's public key and the published information $\{m_w, E, (m_w||E)^{d_0} \bmod N_0\}$ in Step 1 of the Proxy Sharing Phase. And then, the receiver checks the validity of the proxy signature S by computing $S^E \bmod N_0 = (M^D)^E \bmod N_0 = M$ and checking whether M is meaningful or not.

3 Cryptanalysis

3.1 The original signer's forgery

In this section, we show that Hwang et al.'s threshold proxy signature scheme is insecure against the original signer's forgery.

In Hwang et al.'s scheme, the warrant m_w, the proxy signature key D, and the proxy verification key E are constructed by the original signer itself. So, a dishonest original signer can directly generate a valid proxy signature $S^{'}$ on a selected message M, by computing $S^{'} = M^D \bmod N_0$, without other's help. Thus, the forged proxy signature $S^{'}$ will pass the verificatin equation because

$$\begin{aligned}(S^{'})^E \bmod N_0 &= (M^D)^E \bmod N_0 \\ &= M^{d_0^{m_w} e_0^{m_w}} \bmod N_0 = M^{(d_0 \times e_0)^{m_w}} \bmod N_0 \\ &= M,\end{aligned}$$

where $d_0 \times e_0 = 1 \bmod \phi(N_0)$. The proxy signature S by the proxy group and the counterfeit signature $S^{'}$ by the dishonest original signer are indistinguishable. In the other words, the original signer can forge a valid proxy signature easily, and thus Hwang et al.'s scheme does not achieve the proxy-protected property and unforgeability property.

3.2 The general forgery attack

In this section, we show that Hwang et al.'s threshold proxy signature scheme suffers from a general forgery attack.

In Step 3 of the Proxy Sharing Phase, each proxy signer receives $({k_i}^{d_0} \bmod N_0||k_i)^{e_i}$ mod N_i from the original signer, and then decrypts it in order to obtain ${k_i}^{d_0} \bmod N_0$ and k_i. Hwang et al. claimed that each proxy signer can confirm the validity of the partial proxy signing key k_i by checking whether the original signer's signature verification equation $({k_i}^{d_0} \bmod N_0)^{e_0}$ mod $N_0 = k_i$ holds or not. Unfortunately, an attacker can forge it.

We describe this attack as follows:

When the original signer sends $({k_i}^{d_0} \bmod N_0||k_i)^{e_i}$ mod N_i to the proxy signer, a villain can intercept and replace this information by $(k_i^{'} \bmod N_0||K_i)^{e_i} \bmod N_i$, where $k_i^{'}$ is a random number and $K_i = k_i^{'e_0} \bmod N_0$, and then send it to the proxy signer. After receiving the forged information, the proxy signer decrypts and obtains $\{k_i^{'} \bmod N_0, K_i\}$. And then, the proxy signer will confirm the partial proxy signing key K_i using the original signer's public key e_0 because the following equation holds.

$$(k_i^{'} \bmod N_0)^{e_0} \bmod N_0 = k_i^{'e_0} \bmod N_0 = K_i$$

The proxy signer will keep the wrong partial proxy signing key and sign an erroneous partial proxy signature in the event.

Similarly, the proxy signer sends $\{{s_i}^{d_i} \bmod N_i, s_i\}$ to the combiner in Step 1 of the Proxy Signature Issuing Phase. A villain can still forge the partial proxy signature by $\{s_i^{'} \bmod N_i,\ S_i\}$, where $s_i^{'}$ is a random number and $S_i = s_i^{'e_i} \bmod N_i$, and then send it to the combiner. The combiner is ignorant and hence generates a wrong proxy signature.

Note that these weaknesses come from that the primitive RSA signature scheme can not provide authentication of a meaningless message, e.g., a random number. Usually. this problem can be solved by one-way function. Hence, in Hwang et al.'s scheme, their weaknesses can be fixed by modifying $({k_i}^{d_0} \bmod N_0||k_i)^{e_i}$ mod N_i to $(h(k_i)^{d_0} \bmod N_0||k_i)^{e_i}$ mod N_i, and modifying $\{{s_i}^{d_i} \bmod N_i,\ s_i\}$ to $\{h(s_i)^{d_i} \bmod N_i,\ s_i\}$, where $h()$ is an one-way function.

4 Conclusions

In this paper, we cryptanalyze the security of Hwang et al.'s threshold proxy signature scheme. As our analysis, their scheme is insecure against the original signer's forgery. The original signer can create a valid proxy signature, while the proxy group can not deny this proxy signature because the proxy signature satisfies the signature verification equation. Thus Hwang et al.'s scheme does not achieve the proxy-protected property and unforgeability property. Besides, their scheme is also insecure against the general forgery attack. The proxy signer will keep the wrong partial proxy signing key and generate the wrong partial proxy signature, and the combiner will receive wrong partial proxy signatures and generate an erroneous proxy signature. Naturally, we can solve this drawback by using hash function.

References

[1] T. ElGamal, ”Cryptography and logarithms over finite fields,” *Standford University*, CA., UMI Order No. DA 8420519, 119 pages, 1984.

[2] T. ElGamal, ”A public key cryptosystem and signature scheme based on discrete logarithms,” *IEEE Tran. Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[3] M.S. Hwang, J.L. Lu, I.C. Lin, ”A Practical (t,n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem,” *IEEE Trans. Knowledge and Data Engineering*, Vol. 15, Np. 6, pp. 1552-1560, 2003.

[4] L. Harn, ”New digital signature scheme based on discrete logarithm”, *Electronics Letters*, Vol. 30, No. 5, pp. 396-398, 1994.

[5] R.L. Rivest, A. Shamir, and L.M. Adleman, ”A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Comm. ACM*, vol. 21, pp. 120-126, Feb. 1978.

[6] M. Mambo, K. Usuda, and E. Okamoto, ”proxy signature: Delegation of the power to sign messages,” *IEICE Trans. Fundamentals*, Vol. E79-A, No. 9, pp. 1338-1353, 1996.

[7] M. Mambo, K. Usuda, E. Okamoto, ”Proxy signatures for delegating signing operation,” *Proc. of 3rd ACM Conf. on Computer and Communications Security*, pp. 48-57, 1996.

[8] S. Kim, S. Park, and D. Won, ”Proxy signatures, revisited,” *Proc. of International Conf. on Information and Communications Security*, pp. 223-232, 1997.

[9] Hung-Min Sun, N. Y. Lee, and T. Hwang, ”Threshold Proxy Signatures,” *IEE Proceedings - Computers and Digital Techniques*, Vol. 146, No. 5, pp. 259-263, 1999.

[10] Hung-Min Sun, ”An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers,” *Computer Communications*, Vol. 22, No. 8, pp. 717-722, 1999.

[11] Hung-Min Sun, “Convertible Proxy Signature Scheme,” *National Computer Symposium* 1999.

[12] Hung-Min Sun, ”Design of Time-Stamped Proxy Signatures with Traceable Receivers,” *IEE Proceedings - Computers and Digital Techniques*, Vol 147, No. 6, pp. 462-466, 2000.

[13] Hung-Min Sun, “On Proxy Multi-Signature Schemes,” *2000 International Computer Symposium*, Dec. 6-8, 2000.