CRYPTANALYSIS OF LKK PROXY SIGNATURE

Zheng Dong, Shengli Liu , Kefei Chen
Department of Computer Science and Engineering
Shanghai Jiao Tong University Shanghai 200030, P.R.China China[*]
(zheng-dong,liu-sl,chen-kf)@cs.sjtu.edu.cn

Abstract A strong proxy signature scheme [7] based on Schnorr's scheme was proposed by B. Lee *et al.* in 2001. In this paper we show that in the forementioned scheme, original signer may misuse a proxy signer's signature of a message M to forge the proxy signer's normal signature of M.

Keywords: Cryptanalysis, Digital signature, Proxy signature

1. Introduction

Digital signatures play a more and more important role in distributed environment. With digital signature[1,2,3], the transmissions of messages on Internet can achieve authenticity, data-integrity, and non-repudiation. The traditional handwriting are replacing by digital ones. Digital signature schemes can provide the cryptographic services: authentication, data integrity, and non-repudiation. Sometimes, we have the following scenarios: a department manager, say A, is responsible for signing some documents. However, he is busy with other important business, and has no time to sign these documents or he is not in the office upon the time. In those cases, A would like to delegate his signing capability to his secretory, say B, so B would sign documents on behalf of A if A is not available. In the above scenario, we need a so-called proxy signature scheme: a potential signer A delegates his signing capability to a proxy signer, B (in some way, A tells B what kind of messages B can sign), and B signs a message on behalf of the original signer A. the recepient of the message verifies the signature of B and the delegation of A together. Since the concept of proxy signature was introduced by Mambo et al.[4]

[*]Partial funding provided by NSFC under grants 90104005, 60173032 , 60273049 and 60303026 .

in 1996, many proxy signature schemes were proposed [4,5,6,7], all of which are based on Schnorr's signature scheme[3]. According to the undeniability property, the proxy signature schemes are classified into two models: strong proxy signature and weak proxy signature in [7].

- Strong proxy signature: it 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: it represents only original signer's signature. It does not provide non-repudiation of proxy signer.

In [7], B.Lee, H. Kim, and K. Kim also proposed a strong proxy signature scheme, which we will call LKK scheme. In this paper, we will show that LKK scheme is vulnerable to a new attack. In Section II, the brief review of Schnorr's scheme and LKK strong proxy signature scheme are given. Then we describe our new attack against LKK scheme. Section III concludes this paper.

2. Brief review of related schemes and our attack

2.1 Schnorr's scheme [3]

Let us first how Schnorr's digital signature scheme works.

Let p and q be larger primes with $q|p-1$. Let g be a generator of a multiplicative subgroup of Z_p^* with order q, $H(\cdot)$ denotes a collision resistant hash function.

A signer **A** has a private key $x_A \in Z_q^*$ and the corresponding public key $y_A = g^{x_A} \mod p$. To sign a message M, **A** acts as follows:

1 Choose a random $k \in Z_q^*$;

2 Compute $r = g^k \mod p$ and $s = k + x_A H(M,r) \mod q$;

3 Define the signature on M to be the pair (r,s).

The signature is verified by checking that

$$g^s = r y_A^{H(M,r)} \mod p. \tag{1}$$

2.2 LKK strong proxy signature scheme

The following proxy signature scheme has been introduced in [7]. It is based on the above schnorr's scheme.

Suppose that the original signer **A** has a key pair(x_A, y_A), with x_A **A**'s private key and $y_A = g^{x_A} \mod p$ his public key. The (future) proxy signer **B** also has his own key pair (x_B, y_B), with x_B private key and $y_B = g^{x_B} \mod p$ public key.

Generation of the proxy key. The original signer **A** uses Schnorr's scheme to sign warrant information M_ω, which specifies what kind of messages **A** will allow the proxy **B** to sign on his behalf.

More precisely, **A** chooses at random $k_A \in Z_q^*$, and computes $r_A = g^{k_A} \mod p$ and $s_A = k_A + x_A H(M_\omega, r_A) \mod q$, Signer **A** sends (M_ω, r_A, s_A) to proxy signer **B** secretly.

After **B** gets (M_ω, r_A, s_A), he verifies the validity of the Schnorr's signature by checking whether the following equation holds:

$$g^{s_A} = r_A y_A^{H(M_\omega, r_A)} \mod p. \tag{2}$$

If eq.(2) holds, **B** computes his proxy key pair (x_P, y_P) in this way: the private proxy key is

$$x_P = x_B + s_A, \tag{3}$$

and the public proxy key is

$$y_P = g^{x_P} (= y_B r_A y_A^{H(M_\omega, r_A)}) \mod p. \tag{4}$$

Proxy signature generation. In order to create a proxy signature on a message M conforming to the warrant information M_ω, proxy signer **B** uses Schnorr's signature scheme with keys (x_P, y_P) and obtains a signature (r_P, s_P) for the message M. The valid proxy signature will be the tuple $(M, r_P, s_P, M_\omega, r_A)$.

Verification. A recipient can verify the validity of the proxy signature by checking that M conforms to M_ω and the verification equality of Schnorr's signature scheme with public key $y_P (= y_B r_A y_A^{H(M_\omega, r_A)}) \mod p$.

Accept the proxy signature if and only if

$$g^{s_P} = r_P (y_B r_A y_A^{H(M_\omega, r_A)})^{H(M, r_P)} \tag{5}$$

holds.

The authors claimed that the scheme satisfies the following security requirements [7]: strong unforgeability, verifiability, strong identifiability, strong undeniability and prevention of misuse. In next section, we will present a new attack on LKK scheme.

3. Our attack

If the original signer A is dishonest, he can forge the signature of B on message M from a proxy signature.

After obtain the proxy signature $(M, r_P, s_P, M_\omega, r_A)$, the original signer A may forge B's signature on message M as follows:

1 compute $s' = x_A H(M, r_P) \mod q$;

2 compute $s_B = s_P - s' \mod q$, and take $r_B = r_P$.

Then (r_B, s_B) and M satisfy eq. (1), i.e.

$$g^{s_B} = r_B y_B^{H(M,r_B)} \mod p.$$

Suppose that

$$r_B = r_P = g^{k_P} \mod p, \quad s_P = k_P + x_P H(M, r_P) \mod q,$$

where k_P is the random number selected by **B** for proxy signature on M. Then

$$s_B = s_P - s' = k_P + x_B H(M, r_B) \mod q$$

it is obviously that (r_B, s_B) is **B**'s Schonrr signature for message M.

In other words, (M, r_B, s_B) is the forged **B**'s signature on message M.

Remark. J. Herranz et al.[8] claim that other signature schemes (ElGamal signature or DSS) can be used in LKK strong proxy signature scheme. It should be noted that our attack works as well if DSS is used.

4. Summary

Lee et al. briefly modified the proposal of [5] and get a strong proxy signature scheme (LKK scheme)[7]. However, the strong proxy signature scheme has a security flaw. We showed in this paper that in LKK scheme, the original signer **A** is able to misuse his power to forge a proxy signer **B**'s signature for a message, which has been signed by **B** as a proxy signature. Due to the attack, the original signer may confuse his responsibility with the proxy signer's.

References

[1] T.ElGamal, *public key cryptosystem and a signature scheme based on discrete .* IEEE Trans. Inform. Theory, vol. IT-31, pp. 469-472, July 1985

[2] L.Harn, *New digitral signature scheme based on discrete logarithm.* Electron. Lett., vol, no. 5, pp. 296-298, Mar.1994.

[3] C.P. Schnorr, *Efficient signature generation by smart cards.* Journal of Cryptology," vol.4, pp161-174,1991.

[4] M.Mambo, K.Usuda, and E.Okamoto, *Proxy signatures: Delegation of the power to sign messages.* IEICE Trans., 1996, E79-A, (9), pp. 1338-1354.

[5] S.Kim, S.Park, and D.Won, *Proxy signatures, revisited.* Proc. ICICS'97, Int. Conf. Information and Communications Security, 1997,(LNCS), Vol. 1334, pp.223-23

[6] W B Lee, C Y Chang, *Efficient proxy-protected proxy signature scheme based on discrete logarithm*, Proceedings of 10th Conference on Information Security, Hualien, Taiwan, ROC, 2000, pp 4-7

[7] B.Lee, H. Kim, and K. Kim. *Strong proxy signature and its applications.* The 2001 Symposium on Cryptography and Information Security (SCIS 2001) 2001.