Cryptanalysis of New Multisignature Scheme for Specified Group of Verifiers

Yalin Chen
Department of Information Management, National Sun Yat-Sen Unversity 804, Kaohsiung, Taiwan
m924020028@student.nsysu.edu.tw

Chien-Sheng Chen
Department of Computer Science and Information Engineering,
Tunghai UniversityTaichung, 407 Taiwan, R.O.C

Chu-Hsing Lin
Department of Computer Science and Information Engineering,
Tunghai UniversityTaichung, 407 Taiwan, R.O.C
chlin@mail.thu.edu.tw

Jue-Sam Chou
Department of Information Management, Nanhua University Chiayi, 622 Taiwan, R.O.C
jschou@mail.nhu.edu.tw

Abstract

In 2004, Zhang and Xiao proposed a multisignature scheme based on ElGamal discrete logarithm algorithm which allows a signer group to sign a signature and a verifier group to verify the validity of the signed signature. In this paper, we will show that any verifier in the verifier group can break their scheme by replacing the valid signed message with another forged one which will also be authentic according to their scheme.

1. Introduction

A digital signature scheme plays an important role in signing a digital document. For the internet's becoming popular day by day, people rely on digital documents more and more. How to assure that someone has ever agreed upon a negotiated digital document becomes an important issue in the security research field. In other words, we need a mechanism to prove a digital document is worthy of being trusted. A digital signature scheme provides such a desired method. The signer can sign a digital document by his digital signature and it cannot be forged by the other users.

In 1983, Itakura and Nakamura [1] proposed the first multisignature scheme. It let multiple signers collaboratively sign the same message and the resultant multisignature can be verified by a group of verifiers to check whether it is valid or not. Since then, several multisignature schemes have been proposed [2] [3] [4].

In 1999, Harn proposed a multisignature scheme with distinguishable signing authorities [5]. In their scheme, each signer in the group uses his distinguishable signing authority to sign a message collaboratively with other signers in the group. Recently, in 2004, Zhang and Xiao proposed a new multisignature scheme [6] based on both the Harn's scheme [7] and the original ElGamal signature scheme [8]. In their scheme, there is a group of signers signing the multisignature and a group of verifiers checking the validity of the signed signature. Although Zhang and Xiao declare that their scheme can withstand He's attack, we still can find an attack which can break their scheme successfully. We shall describe our attack later on.

The rest of this paper is organized as follows. Section 2 gives a brief review of Zhang - Xiao's scheme. In section 3, we delineate our attack in detail. Finally, a conclusion is given in section 4.

2. Review of Zhang-Xiao's Scheme

In 2004, Zhang and Xiao proposed a multisignature scheme based on ElGamal discrete logarithm. It contains three phases: key generation phase, multisignature generation phase, and multisignature verification phase. We review their scheme briefly as follows:

Key generation phase

Let $G_s = (U_{s_1}, U_{s_2}, ..., U_{s_n})$ be the group of n signers and $G_v = (U_{v_1}, U_{v_2}, ..., U_{v_l})$ be the group of l verifiers. There is a special user called clerk who is trusted in each group respectively. The clerk U_{s_c} in G_s is responsible for verifying all partial signatures sent from each signer in his group and combines those partial signature into a multisignere. The clerk U_{v_c} in G_v assists all verifiers in his group to verify the multisignature. The trusted center generates public values p, q, and g, where p is a large prime number, q is a large prime divisor of $p-1$ and g is an primitive element in Z_p of order q. Let H denote a secure one-way hash function. Each signer U_{s_i} in G_s selects his private key $s_i \in Z_q^*$ and computes the corresponding public key $Y_{s_i} = g^{s_i} \bmod p$. Similarly, each $U_{v_i} \in G_v$ selects his private key $v_i \in Z_q^*$ and computes the corresponding public key $Y_{v_i} = g^{v_i} \bmod p$. Then G_s publishes his group public key computed as $Y_s = \prod_{i=1}^{n} Y_{s_i} \bmod p$ and G_v publishes his group public

key computed as $Y_v = \prod_{j=1}^{l} Y_{v_i} \bmod p$.

Multisignature generation phase

In this phase, G_s generate the multisignature of a message m by performing the following steps:

Step1. Each U_{s_i} selects a random number $k_i \in Z_q^*$ and computes

$$r_i = g^{k_i} \bmod p$$

$$r_i' = Y_v^{k_i} \bmod p$$

then sends r_i and r_i' to the clerk U_{s_c}.

Step2. When U_{s_c} receives all r_i and r_i', he computes

$$r = \prod_{i=1}^{n} r_i \bmod p \text{ and } r' = \prod_{i=1}^{n} r_i' \bmod p$$

then broadcasts r' to all signers in group G_s

Step3. After receiving r', each U_{s_i} computes

$$w_i = s_i(H(m) + r') - k_i \bmod p$$

then sends this partial signature w_i to U_{s_c}.

Step4. After receiving all w_i, U_{s_c} verifies these received partial signatures by

checking whether the equation $Y_{s_i}^{H(m)+r'} = r_i g^{w_i} \bmod p$ holds. If all of them hold, he computes

$$w = \sum_{i=1}^{n} w_i \bmod p$$

then sends message m and its multisignature (r, w) to G_v.

Multisignature verification phase

In this phase, all verifiers in G_v performs the following steps to verify this multisignature:

Step1. Each U_{v_i} in G_v computes a verifying message

$$X_j = r^{v_j} \bmod p$$

and sends X_j to clerk U_{v_c}.

Step2. After receiving all X_j, the clerk U_{v_c} computes

$$X = \prod_{j=1}^{l} X_j \bmod p$$

and broadcasts X to all verifiers in G_v.

Step3. Each verifiers in G_v can verify the multisignature (r, w) of m by checking whether the equation $Y_s^{H(m)+X} = r g^w \bmod p$ holds. If this equation holds, (r, w) is the valid multisignature of m.

3. Our attack

In this section, we demonstrate that how Zhang-Xiao's scheme can be broken by a malicious verifier U_a in G_v. Assume that the signature (r_1, w_1) of m_1 is a valid multisignature signed by G_s. U_a, who now becomes an attacker afrer verifying message m_1 as valid, can perform the following steps to cheat the other verifiers that (r_1, w_1) is also a valid multisignature for a forged message m_2:

Step1. After verifying (r_1, w_1) as a valid multisignature of m_1, from the multisignature verification phase, we know that U_a has both the values of $X_a = r^{v_a} \bmod p$ generated in step 1 and X_1 broadcasted by clerk U_{v_c}. Then he computes

$$X_{v-a} = \prod_{j=1, j\neq a}^{l} X_j = X_1 \cdot X_a^{-1} \bmod p,$$

where X_a^{-1} is the multiplicative inverse of X_a in Z_p.

Step2. U_a computes

$$X' = H(m_1) + X_1 - H(m_2)$$

$$X_a' = X' \cdot X_{v-a}^{-1} \bmod p$$

where X_{v-a}^{-1} is the multiplicative inverse of X_{v-a} in Z_p.

Step3. The attacker U_a sends message m_2 and multisignature (r_1, w_1) to G_v. Then instead of sending $X_a = r^{v_a} \bmod p$, U_a sends X_a' to

U_{v_c} .

Step4. After receiving all X_j , U_{v_c} computes

$$\begin{aligned} X_2 &= \prod_{j=1}^{l} X_j = \prod_{j=1, j\neq a}^{l} X_j \cdot X_a{}' \\ &= \prod_{j=1, j\neq a}^{l} X_j \cdot X' \cdot X_{v-a}{}^{-1} \\ &= X_{v-a} \cdot X' \cdot X_{v-a}{}^{-1} \\ &= X' \end{aligned}$$

then broadcasts $X_2 = X'$ to G_v .

Step5. Each $U_{v_i} \in G_v$ verifies whether (r_1, w_1) is a valid signature of m_2 by the following process.

$$\begin{aligned} Y_s^{H(m_2)+X_2} &= Y_s^{H(m_2)+X'} \\ &= Y_s^{H(m_2)+H(m_1)+X_1-H(m_2)} \\ &= Y_s^{H(m_1)+X_1} \\ &= r_1 g^{w_1} \bmod p \end{aligned}$$

Since $Y_s^{H(m_1)+X_1} = r_1 g^{w_1} \bmod p$ holds. That is, the verification equation can be sstisfied. So, the multisignature (r_1, w_1) is also a valid multisignature of the forged message m_2 . Thus, we have a successful attack.

4. Conclusion

In this paper, in Section 3, we point out the weakness found in Zhang-Xiao's multisignature scheme by showing that how an insider attacker in the verifier group can make a valid multisignature for any forged message. So, Zhang-Xiao's multisignature scheme is not secure enough on the implementation of digital signature system.

References

[1] K. Itakara and K. Nakamura, "A Public Key Cryptosystem Suitable for Digital Multisignatures," NEC Res. Dev. 71 1983, pp. 1-8.

[2] L. Harn and T. Kiesler, "New Scheme for Digital Multisignature," IEEE Electron. Lett. 25 (15), 1989, pp. 1002-1003.

[3] K. Ohta and T. Okamoto, "A Digital Multisignature Scheme Based on The Fiat-Shamir Scheme," ASIACRYPT'91, 1991, pp. 139-148.

[4] T. Wu and S. Chou, "Two ID-based Multisignature Protocols for Sequential and Broadcasting Architecture," Comput. Commun. 19 (10), 1996, pp. 851-856.

[5] L. Harn, "Digital Multisignature with Distinguished Signing Authorities," IEE Electron. Lett. 35 (4), 1999, pp. 294-295.

[6] Z. Zhang and G. Xiao, "New Multisignature Scheme for Specified Group of Verifiers," Applied Mathematics and Computation 157, 2004, pp. 425-431

[7] L. Harn, "New Digital Signature Scheme Based on Discrete Logarithm," IEE Electron. Lett. 30 (5), 1994, pp. 396-398.

[8] T. ElGamal, "A Public-key Cryptosystem and A Signature Scheme Based on Discrete Logarithms," IEEE Trans. Inform. Theory 31 (4), 1985, pp. 469-472.