International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp.49-62
http://dx.doi.org/10.14257/ijsia.2014.8.3.06

Cryptographic Analysis and Improvement of the Structured Multi-Signature Scheme for P2P E-Services

JiYi Wu[1,2], ZhongYou Wang [3*], Jun Zhang[4] and WenJuan Li[1]

[1]*Key Lab of E-Business, Hangzhou Normal University, Hangzhou 310036, China*
[2]*Key Lab of E-business Market Application Technology of Guangdong Province, Guangzhou 510320, China*
[3] *Zhejiang Communications Industry Services Co,Ltd.,Hangzhou 310050, China*
[4]*Department of Computer Science, ShaoXing University, 312000, China*
cloudlab@aliyun.com, zyq@htrdc.com,hellozhangj@foxmail.com, liellie@163.com

Abstract

So far, the trust data storage and transmission security problems are often neglected by researchers in P2P E-Service system. Burmester's scheme and Harn's scheme are two kinds of structured multi-signature schemes. They provided co-signers with different role/position have different management liability and authorization capability. This paper shows some insecurity in these schemes. There are two kinds of attacks on these schemes: (1) the schemes can't resist the dishonest signer forgery attack by forging his own public key (2) everyone can forge some certain messages which to be sign and cannot detect by the signature verifier. Then a new structured signature scheme with verifying signature parameter and all the signers' public keys was proposed. In this way, the new scheme can resist attacks as mentioned, and can be applied to the trust data security transmission in P2P E-Service system.

Keywords: *structured multi-signature, forgery attack, signing order, primitive-root, P2P E-Services*

1. Introduction

In the past ten years, peer to peer network technology develops and becomes more mature, and has become an important technical means to build large-scale E-Service applications. Series of P2P E-Service forms include instant communication, online music, video conference, online games, video on demand, network storage, file sharing, commodities trading, distance education, collaborative design has appeared successively. In order to effectively ensure the safety of all kinds of resources and the transaction process in peer-to-peer systems, we need to introduce information encryption, intrusion detection, authentication, digital signature and other hard security technology, and set social soft security mechanism to fully guarantee fair, trust, at the same time. For hard security issues, the main sources of malicious agents are service requesters, so it can protect service provider. The core idea of soft security is to recognize the existence of a node or a malicious user in the system, and they can break the hard security measures of protection and damage to the normal user. What a user should do is to identify and avoid these malicious nodes, not relying on authority node conditions, only rely on the users themselves and between users of "social control" means. So far, the trust data secure storage and transmission problems are often neglected by researchers, and it's a very difficult thing to find the relevant domestic and foreign literature.

Digital signatures play an important role in our modem electronic society. It is well known

ISSN: 1738-9976 IJSIA

that traditional digital signature allows only one user with a public key and a corresponding private key to sign a message. But, on many occasions, we need to share the responsibility of the signing message with more than one signer. The multi-signature scheme is a special signature scheme, which was first proposed by Itakura and Nakamura in 1983 [1], after that many multi-signature schemes were proposed [2-10]. In some occasions, the signing order of the some multi-signature is fixed, and it can't change discretionarily. Structured multi-signature is a kind of special multi-signature which provided co-signers with different role/position have different management liability and authorization capability. To the structured multi-signatures, not only the group of the signers but also its real signing order is important for verifiers.

In 2000, Burmester and Yvo Desmedt *et al.*, proposed a structured multi-signature extended from an ElGamal-type signature scheme which is based on discrete logarithm problem (DLP) [11]. In 2000, Mitomi and Miyaji proposed two structured multi-signature schemes based on discrete logarithm problem and integer factorization [12]. After that, Yanai construct an new structured multi-signature scheme by utilizing the non-commutative ring homomorphism in a different way, and the new scheme can against various attacks [13]. Then, Wu proposed a new multi-signature from bilinear pairings, the proposed scheme has two properties that it can set up the order of signing in advance and add the intention of signer into the signature [14]. In 2010, Zhang has proposed some structured multi-signature schemes is not secure, then he proposed another structured multi-signature with verifying signature parameter and all the signers' public keys [15]. In 2004, Harn L proposed a structured multi-signature algorithm [16], the size of this scheme is identical to that of an individual signature, and the verification process of the structured multi-signature is almost identical to that of an individual signature.

This paper shows that Burmester's scheme and Harn's scheme had the following weakness: by forging his public key, the dishonest signer can replace some certain signers to sign the message without authority. Anyone can sign the unauthorized message by changing signature parameters. After that, the paper proposes an improved scheme.

The rest of this paper is organized as follows: In Section 2, I briefly review of Burmester's scheme and give out the cryptanalysis on Burmester's scheme. In Section 3, the paper reviews of Harn's structured multi-signature scheme, then gives out one inside attack methods and three kinds of outside attack. The new improved scheme is given out in Section 4. In Section 5 gives discussion and analysis of the new improved scheme. Finally, we draw our conclusions and remarks in Section 6.

2. Security Analysis of Burmester's Scheme

2.1. Briefly Review of Burmester's Scheme [10]

2.1.1. System Initialization

Let p be a large prime, q a prime divisor of p-1, M is the message which to be signed by all the signers, let g be the primitive-root of the cyclic group GF(p), h() denotes a one-way collision resistant cryptographic hash function. Supposed $(U_1, U_2, \cdots\cdots, U_{n-1}, U_n)$ are the signature orders.

For (i=1 to n), All the signers choose an integer $x_i \in Z_q^*$ randomly, as their private keys, then they compute their public keys sequentially as follows:

$$y_1 = g^{x_1} \bmod p,\ y_i = (g.y_{i-1})^x \bmod p \qquad \textbf{(1)}$$

2.1.2. Structured Multi-signature Generation

(1)Signature Parameter R Generation Phase:

①The first signer U_1 randomly chooses an integer $k_1 \in Z_q^*$ and computes $r_1 = g^{k_1} \bmod p$. If gcd(r_1,q)≠1, then chooses new k_1 again.

②For (i=2 to n), the *i*th signer, U_i randomly chooses $k_i \in Z_q^*$ and computes

$$r_i = (r_{i-1})^{x_i}.g^{k_i} \bmod p \quad (2)$$

If $\gcd(r_i, q) \neq 1$, then U_i chooses k_i again until $\gcd(r_i, q) = 1$.

③ R = r_n

(2) Signature generation phase:

①The first signer U_1 computes his signature as follows:

$$s_1 = x_1 + k_1.R.h(R, M) \bmod q \quad (3)$$

Then he sends (s_1,M) to the next signer .

②For (i=2 to n), the *i*th signer U_i firstly checks whether

$$g^{s_{i-1}} \stackrel{?}{=} y_{i-1}.r_{i-1}^{Rh(R,M)} \bmod p \quad (4)$$

If it holds, U_i computes

$$s_i = (s_{i-1} + 1).x_i + k_i.R.h(R, M) \bmod q \quad (5)$$

At last, U_i sends his signature (s_i, M) to the next signer.

2.1.3. Signature Verification

When all the signers have finished signing the message M, the last signer U_n sends (s_n, M) to the signature verifier U_v. U_v checks signature for the message M by the

$$g^{s_n} \stackrel{?}{=} y_n.R^{R.h(R,M)} \bmod p \quad (6)$$

2.2. Cryptanalysis of Burmester's Structured Multi-Signature Scheme

To the multi-signature scheme, there are several possible attacks, which can be divided into outsider attack and insider attack. The outsider attack means that an attacker is not the signature signer, but he can forge multi-signature for some messages. The insider attack means that some malicious signers or one malicious signer can replace some other signers to sign the message, and no one can find someone has forged the signature.

2.2.1. Inside Attack

If U_i is a dishonest signer, he can replace ($U_{t+1}, U_{t+2}, \cdots\cdots, U_i$), (t∈(0,i-1]) to sign the message without authority.

(1)The First Inside Attack Method:

①In system initialization phase, the attacker U_i does not generates his public key firstly, until U_t publishes his public key y_t, then U_i forges his public key $y_i = (y_t.g)^{x_i} \bmod p$.

②In signature parameter R generation phase, U_i chooses $k_i \in Z_q^*$ and forges $r_i = r_t^{x_i}.g^{k_i} \bmod p$ (1≤t≤i-1).

③In signature generation phase, the malicious attackerU_i computes $s_i = (s_t + 1).x_i + k_i.R.h(R, M) \bmod q$.

Proof. Because

$g^{s_i} = g^{(s_t+1).x_i + k_i.R.h(R,M)} \bmod p = (y_t.r_t^{R.h(R,M)})^{x_i}.g^{x_i}.g^{k_i Rh(R,M)} \bmod p = (y_t.g)^{x_i}.(r_t^{R.h(R,M)})^{x_i}.g^{k_i.R.h(R,M)} \bmod p = y_i.(r_t^{x_i}.g^{k_i})^{R.h(R,M)} \bmod p = y_i.r_i^{R.h(R,M)} \bmod p$.

So, if the *i*th signer U_i forges his public key y_i, then he forges r_i, s_i, because $g^{s_i} = y_i.r_i^{R.h(R,M)} \bmod p$, so the Eq.(4) would hold. Hence, anyone cannot find that U_i has forged the signature.

(2)The Second Inside Attack Method:

①U_i forges his public key $y_i = (y_t.g)^{x_i} \bmod p$.

②The attacker U_i forges $r_i = r_t^{x_i} \bmod p$(1≤t≤i-1).

③U_i computes $s_i = (s_t + 1).x_i \bmod q$.

Proof. Because

$g^{s_i} \bmod p = g^{(s_t+1)x_i} \bmod p = (y_t.r_t^{R.h(R,M)})^{x_i}.g^{x_i} \bmod p = (y_t.g)^{x_i}.(r_t^{R.h(R,M)})^{x_i} . \bmod p = y_i.(r_t^{x_i})^{R.h(R,M)} \bmod p = y_i.r_i^{R.h(R,M)} \bmod p$.

(3)The Third Inside Attack Method:

①U_i forges his public key $y_i = y_t^{x_i} \bmod p$.

②U_i randomly selects $k_i \in Z_q^*$, and forges $r_i = r_t^{x_i}.g^{k_i} \bmod p$ (1≤t≤i-1).

③U_i computes $s_i = s_t.x_i + k_i.R.h(R, M) \bmod q$.

Proof. Because

$g^{s_i} \bmod p = g^{s_t.x_i + k_i.R.h(R,M)} \bmod p = (y_t.r_t^{R.h(R,M)})^{x_i}.g^{k_i.R.h(R,M)} \bmod p = y_t^{x_i}.r_t^{x_i.R.h(R,M)}.g^{k_i.R.h(R,M)} \bmod p = y_i.(r_t^{x_i}.g^{k_i})^{R.h(R,M)} \bmod p = y_i.r_i^{R.h(R,M)} \bmod p$.

(4)The Fourth Inside Attack Method:

① U_i forges his public key $y_i = y_t^{x_i} \bmod p$.

②U_i forges $r_i = r_t^{x_i} \bmod p$ (1≤t≤i-1).

③The attacker U_i computes $s_i = s_t.x_i \bmod q$.

Proof. Because

$g^{s_i} \bmod p = g^{s_t.x_i} \bmod p = (y_t.r_t^{R.h(R,M)})^{x_i} \bmod p = y_t^{x_i}.(r_t^{R.h(R,M)})^{x_i} \bmod p = y_i.(r_t^{x_i})^{R.h(R,M)}$

mod p= $y_i.r_i^{R.h(R,M)}$ mod p.

(5)Discussion on these Inside Attack Methods

In the Burmester's structured multi-signature scheme, the verifier does not check all the signers' public keys. So, it gives the chance for all the signer to forge their public key and replace another signers to sign the signature. This paper proposes four inside attack methods to the Burmester's structured signature scheme. In this way, the attacker can replace $(U_{t+1}, U_{t+2}, \cdots\cdots, U_i)$ (t∈[1,i-1]) to sign the message without authority.

Especially if the attacker is the last signer U_n, he can replace all the signers to sign the unauthorized messages by forging his pubic key $y_n = g^{x_n}$ mod p, $R = r_n = g^{k_n}$ mod p, and forge $s_n = x_n + k_n.R.h(R,M)$ mod q. So the Burmester's scheme is not secure.

2.2.2. Outsider Attack

If all the signers sign the message M correctly, it can know that

$$R = g^{(k_n + x_n k_{n-1} + x_n x_{n-1} k_{n-2} + \cdots\cdots + x_n x_{n-1} \cdots x_2 k_1)} \bmod p \qquad (7)$$

From the Eq.(7), we can know, if all the signers ally to forge the system parameter R, they let

$$(k_n + x_n k_{n-1} + x_n x_{n-1} k_{n-2} + \cdots\cdots + x_n x_{n-1} \cdots x_2 k_1) = mq+i \qquad (8)$$

In the Eq.(8) (i ,m are integers, and $1 \le g^i \le q$), so $R= g^i$.

By forging $R= g^i$, everyone can forge all the messages. The outside attack method as follows:

①The attacker can forge all the unauthorized message m', which satisfy h(R,M')= h(R,M)+a (a is an integer)

②The attacker forges the structured multi-signature as follows:

$$s_n' = s_n + iRa \bmod q \qquad (9)$$

Proof Because

$g^{s_n'}$ mod p= $g^{s_n + iRa}$ mod p= $g^{s_n}.g^{iRa}$ mod p= $y_n.R^{Rh(R,M)}.g^{iRa}$. mod p= $y_n.g^{i.R.h(R,M)}.g^{iRa}$ mod p= $y_n.g^{iR(h(R,M)+a)}$ mod p= $y_n.(g^i)^{Rh(R,M')}$ mod p= $y_n.R^{Rh(R,M')}$ mod p.

3. Security Analysis of Harn's Scheme

3.1. Briefly Review of Harn's Scheme [16]

3.1.1. System Initialization

Let p be a large prime, q a prime divisor of p-1, let g be the primitive-root of the cyclic group GF(p), h() denotes a one-way collision resistant cryptographic hash function. Supposed $(U_1, U_2, \cdots\cdots, U_{n-1}, U_n)$ are the signature orders.

All the signers randomly choose their private keys $x_i \in$[1,q-1], then compute their public

keys sequentially as follows:

$$y_{n+1}=g,\ y_i=(y_{i+1})^{x_i} \bmod p. \quad (10)$$

So the system's public key is $y=y_1=g^{x_1.x_2.\cdots.x_n} \bmod p$, and the system private key is $X=x_1.x_2\cdots\cdots x_n \bmod q$.

3.1.2. Structured multi-signature Generation

(1)Signature parameter R generation phase:

①For (i=1 to n), the *i*th signer U_i randomly selects $k_i \in [1,q-1]$, and computes

$$r_i=(y_{i+1})^{k_i} \bmod p\ (1\le i\le n),\ (y_{n+1}=g) \quad (11)$$

②All the signers generates the system parameter

$$R=r_1*r_2*\cdots\cdots*r_n \bmod p \quad (12)$$

(2)Signature generation phase:

①The first signer U_1 generates

$$s_1=x_1.h(M)-k_1R \bmod q \quad (13)$$

②For (i=2 to n), the signer U_{i-1} sends s_{i-1} to U_i, U_i checks whether

$$y_1^{h(M)} \stackrel{?}{=} (r_1.r_2.\cdots\cdots.r_{i-1})^R.(y_i)^{s_{i-1}} \bmod p \quad (14)$$

If it holds U_i computes

$$s_i=s_{i-1}.x_i-k_i.R \bmod q \quad (15)$$

Then U_i sends his signature (s_i, M) to the next signer U_{i+1}.

3.1.3. Signature Verification:

The signature verifier checks the validity of structured multi-signature (s_n,M) for the message M by

$$y_1^{h(M)} \stackrel{?}{=} R^R.g^{s_n} \bmod p \quad (16)$$

If the Eq.(16) holds, it means all the signers sign the message correctly; otherwise, it means someone forges the structured multi-signature, so the signature verifier rejects it.

3.2. Cryptanalysis of the Harn's Scheme

3.2.1. Inside Attack

If U_i is a dishonest signer, he can replace $(U_i,U_{i+1},\cdots\cdots U_n)$ to sign the message without authority.

①The attacker U_i forges his public key

$$y_i=g^{x_i} \bmod p \quad (17)$$

②For (f =i to n), the attacker U_i randomly selects $\{k_i,k_{i+1},\cdots\cdots,k_n\} \in [1,q-1]$, and forges

$$r_f=g^{k_f} \bmod p\ (i\le f\le n) \quad (18)$$

③When the attacker U_i received (s_{i-1},M), the attakcer forges

$$s_n = x_i.s_{i-1} - (k_i + k_{i+1} + k_{i+2} + \cdots\cdots + k_n) * R \mod q \qquad \textbf{(19)}$$

Proof. $y_1^{h(M)} = R^R.g^{s_n} \mod p$.

In this forge attack method $(U_1, U_2, \cdots\cdots U_{i-1})$ are honest signers, U_i is an attacker, who can replace $(U_i, U_{i+1}, \cdots\cdots U_n)$ to sign the message without authority

$$\begin{cases} y_f = (y_{f+1})^{x_f} \mod p = (y_{f+2})^{x_f x_{f+1}} \mod p = \cdots = g^{(x_f x_{f+1} \cdots x_i)} \mod p & (1 \le f \le i-1) \\ y_f = g^{x_f} \mod p & (f=i) \end{cases}$$

$$\begin{cases} r_f = (y_{f+1})^{k_f} \mod p = g^{k_f x_{f+1} x_{f+2} \cdots x_i} \mod p & (1 \le f \le i-1) \\ r_f = g^{k_f} \mod p & (i \le f \le n) \end{cases}$$

So $R = \prod_{i=1}^{n} r_i \mod p = g^{k_1 x_2 x_3 \cdots x_i}.g^{k_2 x_3 x_4 \cdots x_i}.\cdots\cdots.g^{k_i}.g^{k_{i+1}} \cdots\cdots.g^{k_n} \mod p$

$s_{i-1} = s_{i-2}.x_{i-1} - k_{i-1}.R \mod q = (s_{i-3}.x_{i-2} - k_{i-2}.R).x_{i-1} - k_{i-1}.R \mod q$

$= s_{i-3}.x_{i-1}.x_{i-2} - x_{i-1}.k_{i-2}.R - k_{i-1}.R \mod q = \cdots\cdots = h(M)\prod_{f=1}^{i-1} x_f - k_1.R.\prod_{f=2}^{i-1} x_f - \cdots - x_{i-1}.k_{i-2}.R - k_{i-1}.R \mod q.$

Hence $s_n = x_i.s_{i-1} - (k_i + k_{i+1} + \cdots\cdots + k_n).R \mod q = h(M)\prod_{f=1}^{i} x_f - (k_1\prod_{f=2}^{i} x_f + k_2\prod_{f=3}^{i} x_f + \cdots\cdots + x_i.x_{i-1}.k_{i-2} + x_i.k_{i-1}).R - (k_i + k_{i+1} + \cdots\cdots + k_n).R \mod q.$

And $R^R.g^{s_n} = R^R.g^{(h(M)\prod_{f=1}^{i} x_f - (k_1\prod_{f=2}^{i} x_f + k_2\prod_{f=3}^{i} x_f + \cdots + x_i k_{i-1})R - (k_i + k_{i+1} + \cdots + k_n)R)} =$

$R^R.g^{((h(M)\prod_{f=1}^{i} x_f - (k_1\prod_{f=2}^{i} x_f + k_2\prod_{f=3}^{i} x_f + \cdots + x_i k_{i-1})R - (k_i + k_{i+1} + \cdots + k_n)R)} \mod$

$p = R^R.y_1^{h(M)}/((g^{k_1\prod_{f=2}^{i} x_f}.g^{k_2\prod_{f=3}^{i} x_f}.\cdots\cdots.g^{x_i k_{i-1}})^R.(g^{k_i}.\cdots\cdots g^{k_n})^R) \mod$

$p = R^R.y_1^{h(M)}/((r_1.r_2.\cdots r_{i-1})^R.(r_i.r_{i+1}.\cdots r_n)^R) \mod p = y_1^{h(M)} \mod p.$

So the Eq.(16) will hold. Hence the attacker U_i can replace $(U_i, U_{i+1}, \cdots\cdots U_n)$ to sign the message by forging his public key. The Harn's structured multi-signature scheme is similar to the Burmester's scheme, the verifier does not verify all the signers' public key, so it gives some malicious signers to forge the signature.

Especially, If U_1 is a malicious attacker, he can replace all the signers to forge any messages M by following:

①The malicious attacker U_1 randomly selects $x_1 \in [1,q-1]$, and computes his public key

$$y_1 = g^{x_1} \bmod p \quad (20)$$

②U_1 randomly selects $\{k_1, \cdots\cdots, k_n\} \in [1,q)$, and for(i=1 to n) he computes

$$r_i = g^{k_i} \bmod p,\ R = \prod_{i=1}^{n} r_i \quad (21)$$

③The malicious attacker U_1 forges the structured multi-signature

$$s_n = x_1.h(M) - (k_1 + k_2 + \cdots\cdots + k_n).R \bmod q \quad (22)$$

Proof. Because

$y_1^{h(M)} \bmod p = g^{x_1 h(M)} \bmod p = g^{x_1 h(M)}.g^{(k_1+k_2+\cdots\cdots+k_n).R} / g^{(k_1+k_2+\cdots\cdots+k_n).R} \bmod p = g^{x_1 h(M)-(k_1+k_2+\cdots+k_n)R}.(r_1.r_2.\cdots.r_n)^R \bmod p = R^R.g^{s_n} \bmod p.$

The Eq.(16) $y_1^{h(M)} = R^R.g^{s_n} \bmod p$ would hold. So, if the first signer U_1 is the malicious attacker, who can replace all the signers to sign the message. And because the Eq.(16) holds, anyone cannot find that U_1 has forged the signature.

3.2.2. Outside Attack

(1) The First Outside Attack Method:

The attacker can forge some certain messages after the attacker know a valid signature (R, s_n ,M):

①The attacker can forge an unauthorized message m', which satisfy $h(m') = h(M).g^a$ (a is an integer)

②The attacker sets

$$R' = g^a.R \bmod p,\ s_n' = g^a(s_n - a.R) \bmod q. \quad (23)$$

Proof $y_1^{h(m')} = g^{s_n'}.R'^{R'} \bmod p$

$y_1^{h(m')} \bmod p = y_1^{h(M).g^a} \bmod p = (g^{s_n}.R^R)^{g^a} \bmod p = g^{s_n g^a}.R^{Rg^a} \bmod p = g^{s_n g^a}.(g^a R)^{g^a R} / (g^a)^{g^a R} \bmod p = g^{s_n g^a - a g^a R}.(g^a R)^{g^a R} \bmod p = g^{g^a(s_n - aR)}.(g^a R)^{g^a R} \bmod p = g^{s_n'}.R'^{R'} \bmod p.$

(2)The Second Outside Attack Method:

①The attacker can forge an unauthorized message m', which satisfy $h(m') = y_1^a(h(M) + a.R)$ (a is any integer)

②The attacker sets

$$R' = y^a.R \bmod p,\ s_n' = y_1^a.s_n \bmod q \quad (24)$$

Proof. Because

$y_1^{h(m')} \bmod p = y_1^{y_1^a.(h(M)+a.R)} \bmod p = y_1^{h(M).y_1^a}.y_1^{y_1^a.a.R} \bmod p = (g^{s_n}.R^R)^{y_1^a}.y_1^{y_1^a.a.R} \bmod p = g^{s_n.y_1^a}.(R^R.y_1^{a.R})^{y_1^a} \bmod p = g^{s_n.y_1^a}.(R.y_1^a)^{R.y_1^a} \bmod p = g^{s_n'}.R'^{R'} \bmod p.$

(3)The Third Method of Outside Attack:

It can know that $r_f = g^{x_n \cdot x_{n-1} \cdot \cdots \cdot x_{f+1} \cdot k_f} \mod p$. So

$$R = \prod_{i=1}^{n} r_i \mod p = g^{(k_n + x_n k_{n-1} + x_n x_{n-1} k_{n-2} + \cdots\cdots + x_n x_{n-1} \cdots x_2 k_1)} \mod p \quad (25)$$

From the Eq.(25), we can know, if all the signers ally to forge R, they set

$$k_n + x_n k_{n-1} + x_n x_{n-1} k_{n-2} + \cdots\cdots + x_n x_{n-1} \cdots x_2 k_1 = mq+i \quad (26)$$

In the Eq.(26), i ,m are integers, and $1 \le g^i \le q$. So $R = g^i$, in this way everyone can forge a lot of messages as follows:

(1) The attacker can forge an unauthorized message, which satisfy h(m')= h(M).a (a is a integer)

(2) The attacker sets

$$s_n' = s_n.a + i.R.(a-1) \mod q \quad (27)$$

Proof. Because

$y_1^{h(m')} \mod p = y_1^{h(M)a} \mod p = g^{s_n a}.R^{Ra} \mod p = g^{s_n a}.g^{iRa} \mod p = g^{s_n a}.g^{iR}.g^{iRa} / g^{iR} \mod p = g^{s_n a}.g^{iR}.g^{iRa-iR} \mod p = g^{s_n a + iR(a-1)}.g^{iR} \mod p = g^{s_n}.R^R \mod p$.

(4)Discussion on the Outside Attacks Methods

If the attacker only knows single valid signature, there are no risks associated with the first outside attack method and the second outside attack method. Because there are few messages m', which satisfy h(m')= h(M) g^a or satisfy h(m')= y_1^a (h(M)+aR), and it is almost impossible that the unauthorized message is meaningful. But if the attacker know a lot of valid signature $\{(\{(R_1, s_{n1}, M_1), (R_2, s_{n2}, M_2), \cdots\cdots, (R_k, s_{nk}, M_k)\}$, or g is not a large integer (g is the primitive-root of the cyclic group GF(p)). Supposed the attacker collects k valid signatures, and k>= $\sqrt{g}$, from the birthday attack, these methods are serious hazard.

The third outside attack method is more dangerous than other outside attack methods. In the third method, the attacker can forge a lot of unauthorized messages which satisfy h(m')= h(M)*a. If h(m')/h(M) is an integer, the attacker set $s_n' = s_n.a + i.R.(a-1) \mod q$. If h(m')/h(M) is a decimal, and if $s_n.a + i.R.(a-1)$ is also an integer, the outside is really effective too.

4. A New Structured Multi-signature Scheme

4.1. System Initialization

Let p be a large prime, q a prime divisor of p-1, let g be the primitive-root of the cyclic group GF(p), h() denotes a one-way collision resistant cryptographic hash function. Supposed $(U_1, U_2, \cdots\cdots, U_{n-1}, U_n)$ are the signature orders.

All the signers randomly choose their private keys $x_i \in Z_q^*$, compute their public keys sequentially as follows:

$$y_1 = g^{x_1} \mod p, \quad y_i = y_{i-1}^{x_i} \mod p \quad (28)$$

Then the system public key of ordered group $(U_1, U_2, \cdots\cdots, U_{n-1}, U_n)$ is set to $y = y_n = g^{x_1 \cdot x_2 \cdot \cdots \cdot x_n} \bmod p$, and the system private key is $X = x_1 . x_2 . \cdots\cdots . x_n \bmod q$.

When the signer finish generating their public key and private key, the system verifier check the signers' public keys are forgery or not. As the sample of checking U_i' public key by following ways:

(1) The system verifier U_v randomly chooses $t_i \in Z_q^*$ （1≤i≤n） to the signer U_i, and computes

$$j_i = (y_{i-1})^{t_i} \bmod p \quad (29)$$

After that, U_v publishes U_i' parameter j_i.

(2) When the signer U_i receives j_i he computes

$$w_i = j_i^{x_i} \bmod p \quad (30)$$

Then U_i sends w_i to the system verifier U_v.

(3)The system verifier U_v receives w_i, he checks U_i' public key by

$$w_i \stackrel{?}{=} (y_i)^{t_i} \bmod p \quad (31)$$

In this method, the system verifier U_v can check all the singers' public keys are forgery or not, if all the signers' public keys are not forgery, the signature continued, else reject the signature.

4.2 Structured Multi-signature generation

4.2.1 Signature Parameter R Generation Phase:

①For (i=1 to n), the *i*th signer U_i randomly selects $k_i \in Z_q^*$, and computes

$$r_1 = g^{k_1} \bmod p,\ r_i = (r_{i-1})^{x_i} . g^{k_i} \bmod p\ (2 \le i \le n) \quad (32)$$

If gcd(r_i,q)≠1, then U_i selects new k_i and computes r_i again.

②R = r_n Where gcd (R, q) ≠ 1.

4.2.2 Generation of Signature:

①The first signer U_1 computes his structured multi-signature

$$s_1 = x_1 + k_1 . h(R, M) \bmod q \quad (33)$$

②For (i=2 to n), the signer U_{i-1} sends s_{i-1} to U_i, then U_i checks that

$$g^{s_{i-1}} \stackrel{?}{=} y_{i-1} . r_{i-1}^{h(R,M)} \bmod p \quad (34)$$

Then U_i computes

$$s_i = s_{i-1} . x_i + k_i . h(R, M) \bmod q \quad (35)$$

If U_i is the last signer, he sends the structured multi-signature s_n; otherwise he sends s_i to the next signer U_{i+1}.

4.3. Signature Verification

When all the signers have finished signing the message M, the last signer U_n sends (s_n, M) to the signature verifier U_v, U_v checks the validity of structured multi-signature for the message M by the following equality:

$$\begin{cases} g^{s_n} \stackrel{?}{=} y_n . R^{h(R,M)} \bmod p \\ R<p \text{ and } R \bmod p \neq 0 \end{cases} \quad (36)$$

If the Eq.(36) would hold, it means that all the signers sign the message correctly, and they doesn't allay to forge signature (the outside attack is impossible), so the verifier U_v accepts the structured multi-signature; otherwise it means some signers have forged the signature, or someone disturbs the signature, so U_v must let all the signers sign the message again until the Eq.(36) holds.

5. Discussion

5.1. Impossible of Inside Attack

In the Burmester's structured multi-signature scheme and Harn's scheme, because the signature does not verify all the signers' public key. So, it gives some opportunities to forge their public keys. Therefore, some dishonest signers can replace other signers to sign the message.

The new scheme can prevents a signer forging his public key $y_i = g^{x_i} \bmod p$ by judging the signer's public key $w_i = j_i^{x_i} \bmod p = (y_{i-1})^{t_i x_i} \bmod p = (y_{i-1})^{x_i t_i} \bmod p = (y_i)^{t_i}$. If U_i want to forges the message, first, he must forge his public key and let the equation $w_i = j_i^{x_i} \bmod p$, it must satisfy the equation $(x_1 . x_2 . \cdots \cdots . x_{i-1}) t_i = kq$ (k is an integer). Because q is a very large prime, and t_i is the signature verifier U_v's private key, so all the signers cannot know t_i and get the correct value of q. It is almost impossible to satisfy $(x_1 . x_2 . \cdots \cdots . x_{i-1}) t_i = kq$, so the signer's inside attack is impossible. Therefore, with public key verifying, the new scheme can resist inside forge attack.

5.2. Impossible of Outside Attack

The new scheme uses discrete logarithm problem (DLP) to ensure its security. So, if an attacker who is not the signer but he wants to generate or forge a structured multi-signature for some messages by direct crack attack, he should compute s_n with the Eq.(36) $g^{s_n} \stackrel{?}{=} y_n . R^{h(R,M)} \bmod p$. Until now, it is impossible, because computing s_n is the difficulty in solving the discrete logarithm problem (DLP). And it is also impossible to compute the signers' private keys x_i by their public keys $y_1 = g^{x_1} \bmod p$, $y_i = y_{i-1}^{x_i} \bmod p$. Hence, anyone cannot resist direct crack to the new structured multi-signature.

And the new signature schemes can resist the outside attack as above mentioned. In the new scheme, the signature verifier checks signature $g^{s_n} \stackrel{?}{=} y_n.R^{h(R,M)}$ mod p and judging R<p and R mod p≠0. Hence, if anyone wants to use outside attack to the new scheme, R would>=p, and R mod p. By checking the system parameter R, it can resist outside attack method.

So the new structured multi-signature scheme can avoid a lot of inside attacks and outside attacks with checking all the signers' public keys and signature parameter R.

6. Conclusions

This paper shows that the classic structured multi-signature scheme such as Burmester's and Harn's schemes are not secure, because they can not resist inside attack and outside attack. To the Burmester's scheme, if U_i is the attacker, he can replace $(U_{t+1}, U_{t+2}, \cdots\cdots, U_i)$ (t∈[0,i-1]) to sign the message without authority, and if the signature parameter R takes a certain value, anyone can forge all the messages. To the Harn's scheme, if U_i is the attacker, he can replace $(U_i, U_{i+1}, \cdots\cdots U_n)$ to sign the message without authority, and anyone can forge a certain of messages. Then this paper propose a new structured multi-signature scheme with verifying R and all the signers' public keys, which can resist the attacks as above mentioned. In this way, the new scheme can be applied to the trust data security transmission in P2P E-Service system [17-18].

Acknowledgements

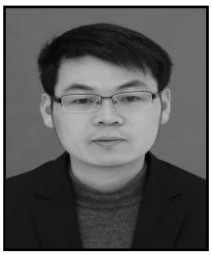
This work is supported by the National Natural Science Fund of China (NO.61379034), the Natural Science Fund of Zhejiang Province (NO.LQ12G02016, LQ12F02006), the open fund for Key Lab of E-business Market Application Technology of Guangdong Province (2011GDECOF07).

References

[1] K. Itakura and K. Nakamura, "A public key cryptosystem suitable for digital multi-signature", NEC Res and Develop, vol. 71, no. 10, **(1983)**, pp. 1- 8.
[2] S. Zuhua, "Improvement of identity-based proxy multi-signature scheme", Journal of Systems and Software, vol. 82, no. 5, **(2009)**, pp. 794-800.
[3] S.-J. Hwang and Y.-H. Lee, "Repairing ElGamal-like multi-signature schemes using self-certified public keys", Applied Mathematics and Computation, vol. 156, no. 08, **(2004)**, pp. 73-83.
[4] S. Ying, X. Chunxiang, Y. Yong and Y. Bo, "Improvement of a proxy multi-signature scheme without random oracles", Computer Communications, vol. 34, no. 3, **(2011)**, pp. 257-263.
[5] B. Wang, "On the security of an identity-based proxy multi-signature scheme", IET Information Security, vol. 4, no. 2, **(2010)**, pp. 45-48.
[6] M. Changshe, W. Jian, Y. Li and D. Robertm, "Efficient discrete logarithm based multi-signature scheme in the plain public key model. Des Codes Cryptography", vol. 54, no. 2, **(2010)**, pp. 121-133.
[7] F. Cao and Z. Cao, "A secure identity-based proxy multi-signature scheme", Information Science, vol. 179, no. 01, **(2009)**, pp. 292-302.
[8] W.Qin and C. Zhenfu, "Identity based proxy multi-signature", Journal of Systems and Software, vol. 80, no. 7, **(2007)**, pp. 1023-1029.
[9] Y. Sunghyun, L. Heuiseok, J. Young-Sik, J. Soonyoung and C. Jae-Khun, "The biometric based convertible undeniable multi-signature scheme to ensure multi-author copyrights and profits", Wireless Personal Communications, vol. 60, no. 3, **(2011)**, pp. 405-418.
[10] Q. Haifeng and X. Shouhua, "Non-interactive multisignatures in the plain public-key model with efficient verification", Information Processing Letters, vol. 111, no. 2, **(2010)**, pp. 82-89.

[11] T.-S. Wu, H.-Y. Lin and M.-J. Shiu, "Threshold multi-proxy multi-signature scheme based on bilinear pairings", WSEAS Transactions on Information Science and Applications, no. 04, **(2007)**, pp. 1393-1399.
[12] Y. Naoto, C. Eikoh and M. Masahiro, "A secure structured multisignature scheme based on a non-commutative ring homomorphism", IEICE Trans Fund Electron Commun Comput Sci, vol. E94-A, no. 6, **(2011)**, pp. 1346-1355.
[13] M. Burmester, Y. Desmedt, H. Doi, M. Mambo, E. Okamoto, M. Tada and Y. Yoshifuji, "A structured ElGamal-Type multisignature scheme", Advances in Cryptology-Proceedings of PKC'2000, **(2000)**, pp. 466-482.
[14] W. Ke-Li, W. Bin, W. Xiang-He and L. Feng-Yu, "Structured multi-signature scheme with signers' intentions", Journal of Electronics and Information Technology, vol. 28, no. 5, **(2006)**, pp. 823-826.
[15] Z. Jun, "Cryptographic analysis of the two structured multi-signature schemes", Journal of Computational Information Systems, vol. 6, no. 9, **(2010)**, pp. 3127-3135.
[16] L. Harn, L. Cy and T. C. Wu, "Structured multisignature algorithms", IEE Proceedings Computers and Digital Techniques, vol. 153, no. 3, **(2004)**, pp. 231-234.
[17] W. Jiyi, Z. Jianlin, W. Tong and S. Qianli, "Study on Redundant Strategies in Peer to Peer Cloud Storage Systems", Applied Mathematics & Information Sciences, vol. 5, no. 2, **(2011)**, pp. 235S-242S.
[18] W. Ji-yi, F. Jian-qing, P. Ling-di and X. Qi, "Study on the P2P Cloud Storage System", Acta Electronica Sinica, vol. 39, no. 5, **(2011)**, pp. 1100-1107.

Authors



JiYi WU is an associate professor at the Key Lab of E-Business, Hangzhou Normal University. He received PhD degree in 2011 from Zhejiang University, Hangzhou China, in computer science. His research interests include services computing, trust and reputation. He has published more than 20 journal articles indexed by SCI, EI.

ZhongYou WANG is the deputy director at Technology R & D Center of Zhejiang Communications Industry Services Co,Ltd. He received Master's Degree in computer science in 2009 at Hangzhou Dianzi University. His research interests include service trust and security, software engineering.

Jun ZHANG was born in 1979. He is an associate professor at the department of computer science, ShaoXing University,China. His research interests include network security, trust and reputation. He has published more than 20 journal articles indexed by SCI,EI.

WenJuan LI was born in 1978. She is a lecturer at Hangzhou Normal University. She received PhD degree in 2011 from Zhejiang University, Hangzhou China, in computer science. Her research interests include cloud computing, trust and reputation. She has published more than 10 journal articles indexed by SCI, EI.