INSIDER FORGERY ATTACKS ON WANG-LIN-CHANG THRESHOLD SIGNATURE SCHEMES WITH TRACEABLE SIGNERS

Chien-Lung Hsu and Tzong-Chen Wu

Department of Information Management,
National Taiwan University of Science and Technology,
Taipei, Taiwan 106, Republic of China
Email: {d8609004, tcwu}@cs.ntust.edu.tw

ABSTRACT

Wang, Lin and Chang (1998) proposed two threshold signature schemers, one is with a mutually trusted center and the other is not, that provide the ability to trace back who the participant signers are involved in the construction of the group signature for a given message if necessary. Lately, Tseng and Jan (1999) demonstrated two outsider forgery attacks on the Wang-Lin-Chang schemes. In this paper, we will demonstrate two insider forgery attacks on the Wang-Lin-Chang schemes. That is, any malicious participant signer can successfully forge a valid group signature for an arbitrarily chosen message by himself.

1. INTRODUCTION

In a (t, n) threshold signature scheme, any t out of n members of a group can be on behalf of the group to generate a group signature for a given message, such that any verifier can verify the group signature with only knowing the public key associated to the group, not necessarily to know the public keys for all participant signers [1, 2]. A threshold signature scheme provides anonymity for the participant signers, since only the public key of the group is required for signature verification. This makes the threshold signature schemes more applausive to group-oriented applications [2].

Recently, Wang, Lin and Chang [7] proposed two threshold signature schemes based on the intractability of the discrete logarithm problem [3, 4], one is with the assistance of a mutually trusted and the other is not. Both the Wang-Lin-Chang schemes provide the ability to trace back who the participant signers are involved in the construction of a group signature for a given message if necessary. Lately, Tseng and Jan [6] showed that the Wang-Lin-Chang schemes are vulnerable to the outsider forgery attacks. That is, an outsider of the signing group could use any previously generated group signature to forge a valid group signature for an arbitrarily chosen message without knowing the group members' private keys. In this paper, we will show that both the Wang- Lin-Chang schemes are also vulnerable to the insider forgery attacks. That is, any malicious participant signer can successfully forge a valid group signature for an arbitrarily chosen message by himself.

In the subsequent sections, we first give a brief review of the Wang-Lin-Chang schemes, and then demonstrate how the insider forgery attacks on the Wang-Lin-Chang schemes can work.

2. REVIEW OF WANG-LIN-CHANG SCHEMES

There are three roles required in the system: a system authority (SA), a mutually trusted center (MTC), and a designated trusted clerk (CLK). The task for SA is to define necessary public parameters for system setup. The task for MTC is to generate a private/public key pair for each member of the signing group. CLK is responsible for the verification of individual signature and the construction of a group signature from the verified individual signatures. In the following, two threshold signature schemes proposed by Wang, Lin and Chang are described. The first threshold signature scheme works with the assistance of a MTC, whereas the second threshold signature scheme works without the assistance of a MTC.

2.1 Threshold Signature Scheme with MTC

For system setup, SA defines the following public parameters $\{P, P', Q, g, \alpha, H\}$, where P is a large prime, P' is a large prime factor of $P-1$, Q is a large prime factor of $P'-1$, g and α are two generators with order P' and Q over GF(P) and GF(P'), respectively, and H is a one-way hash function. It is assumed that H is collision-free.

Let $G=\{u_1, u_2, ..., u_n\}$ be the group of n signers, where any t out of n signers can be on behalf of G to generate a group signature for a given message. Denote v_i as the identity for u_i. Upon receiving the registration request submitted by the members of G, MTC first randomly generates a $(t-1)$-degree polynomial $f(v) = a_0 + a_1 \cdot v + ... + a_{t-1} \cdot v^{t-1} \bmod Q$, where $a_i \in Z_Q$ (for i = 0,1,...,$t-1$), and then generates a private/public key pair (x_i, y_i) for each $u_i \in G$ and a private/public key pair (X, Y) for G, where

$x_i = \alpha^{f(v_i)} \bmod P'$ and $y_i = g^{\alpha^{f(v_i)}} \bmod P$,

$X = f(0)$ and $Y = g^{\alpha^X} \bmod P$.

After that, MTC sends x_i to u_i (for $i = 1,2,...,n$) secretly and publishes Y and all y_i's. Note that MTC does not need to keep the private key X secretly after the initialization stage, because it can be dynamically constructed by any t out of n participant signers in G during the generation of a group signature. Also note that any participant signer in G does not have any useful knowledge about X during the group signature generation stage.

Without loss of generality, let $T = \{u_1, u_2, ..., u_t\}$ be t members of G that want to collaboratively sign a message M. Let $L_i = \prod_{i \neq j, j=1}^{t} -v_j \cdot (v_i - v_j)^{-1} \bmod Q$. For signing M on behalf of G, each $u_i \in T$ first randomly chooses two integers $d_i \in Z_Q^*$ and $k_i \in Z_{P'}^*$, and then computes

$r_{i1} = \alpha^{d_i} \bmod P'$ and $s_{i1} = (x_i)^{L_i} \cdot H(M) \cdot r_{i1} \bmod P'$,

$r_{i2} = g^{k_i} \bmod P$ and $s_{i2} = k_i^{-1} \cdot (s_{i1} - x_i \cdot r_{i2}) \bmod P'$.

Finally, u_i sends $(M, r_{i1}, s_{i1}, r_{i2}, s_{i2})$ to CLK for constructing a group signature of M. Here, (s_{i1}, r_{i2}, s_{i2}) is regarded as an individual signature of M signed by u_i.

Upon receiving $(M, r_{i1}, s_{i1}, r_{i2}, s_{i2})$ sent from u_i, CLK first verifies the individual signature (s_{i1}, r_{i2}, s_{i2}) by testing if

$$g^{s_{i1}} = y_i^{r_{i2}} \cdot {r_{i2}}^{s_{i2}} \pmod P. \quad (1)$$

When all individual signatures sent from these t participant signers are successfully verified, CLK constructs a group signature (R, S) of M for G, where

$R = \prod_{i=1}^{t} r_{i1} \bmod P'$ and $S = \prod_{i=1}^{t} s_{i1} \bmod P'$.

Meanwhile, CLK also publishes a $(t-1)$-degree polynomial

$h(y) = \Sigma_{i=1}^{t} v_i \cdot \Sigma_{j=1, j \neq i}^{t} (y - y_j) \cdot (y_i - y_j)^{-1} \bmod P$.

The polynomial $h(y)$ is used for the purpose of tracing back who the participant signers are involved in the construction of a group signature on behalf of G.

Any verifier with only knowing the group public key Y can verify the group signature (R, S) of M by testing if

$$g^S = Y^{(H(M))^t \cdot R} \pmod P. \quad (2)$$

If necessary, the verifier can further find out who the participant signers are involved in the construction of the group signature (R, S) by testing if $h(y_i) = v_i$ (for $i = 1,2,...,n$). It the equality holds, then the member u_i with the public key y_i is one of the participant signers.

2.2 Threshold signature scheme without MTC

This scheme use the same system parameters defined in the previous subsection. After the system parameters are defined, each member of G not only generates a private/public key pair for himself but also for every other member in the same group. To act as an MTC, each $u_i \in G$ first randomly generates a $(t-1)$-degree polynomial $f_i(v)$, and then generates a private/public key pair (x_i, y_i) for himself and a private/public key pair (x_{ij}, y_{ij}) for every other member u_j in G, where

$x_i = \alpha^{f_i(0)} \bmod P'$ and $y_i = g^{\alpha^{f_i(0)}} \bmod P$,

$x_{ij} = \alpha^{f_i(v_j)} \bmod P'$ and $y_{ij} = g^{x_{ij}} \bmod P$.

After that, all members in G form as an ordered ring and then collaboratively generate a group public key $Y = g^{\prod_{i=1}^{t} f_i(0)} \bmod P$ for G. Finally, u_i sends x_{ij} secretly to u_j and publishes all y_{ij}'s (for $j = 1,2,...,n$ and $i \neq j$).

For signing M on behalf of G, each $u_i \in T$ first randomly chooses two integers $d_i \in Z_Q^*$ and $k_i \in Z_{P'}^*$, and then computes

$r_{i1} = \alpha^{d_i} \bmod P'$ and

$s_{i1} = (x_i \cdot \prod_{k=t+1}^{n} \alpha^{f_k(v_i) \cdot L_i}) \cdot H(M) \cdot r_i \bmod P'$,

$r_{i2} = g^{k_i} \bmod P$ and

$s_{i2} = k_i^{-1} \cdot (s_{i1} - x_i \cdot r_{i2}) \bmod P'$.

Finally, u_i sends $(M, r_{i1}, s_{i1}, r_{i2}, s_{i2})$ to CLK for constructing a group signature of M. Again, (s_{i1}, r_{i2}, s_{i2}) is regarded as an individual signature of M signed by u_i, and can be verified through the equality test of Equation 1. As done in the scheme with MTC, CLK constructs a group signature (R, S) of M for G from all verified individual signatures (s_{i1}, r_{i2}, s_{i2})'s, and (M, R, S) can be verified through the equality test of Equation 2. Meanwhile, CLK also publishes $(t-1)$-degree polynomials

$h_j(y) = \Sigma_{i=1}^{t} v_i \cdot \prod_{l=1, l \neq i}^{t} y - y_{jl}) \cdot (y_{ji} - y_{jl})^{-1} \bmod P$

(for $j = 1,2,...,t$).

The polynomials $h_j(y)$'s are used for the purpose of tracing back who the participant signers are involved in the construction of a group signature on behalf of G.

As to find out who are the participant signers involved in

the construction of the group signature (R,S), any verifier can test if $h_j(y_{ji}) = v_i$ (for $i = 1,2,...,n$). It the equality holds, then the member u_i with the public key y_{ji} is one of the participant signers.

3. INSIDER FORGERY ATTACKS ON WANG-LIN-CHANG SCHEMES

Without loss of generality, let $T = \{u_1, u_2, \cdots, u_t\}$ be t participant signers on behalf of G to sign a message M. Consider the case that a malicious participant signer u_w in T wants to forge a valid group signature for a chosen message M' (not agreed to all participant signers in T) during the construction of a group signature (R,S) for M (agreed to all participant signers in advance). In the following, we will demonstrate two scenarios to show how can u_w successfully plot such attack on the Wang-Lin-Chang schemes, respectively.

An insider forgery attack on the Wang-Lin-Chang scheme with MTC – During the construction of an individual signature, u_w first randomly selects two integers $d_w \in Z_Q^*$ and $k_w \in Z_{P'}^*$, and then computes $(r_{w1}, s_{w1}, r_{w2}, s_{w2})$, where

$r_{w1} = \alpha^{d_w} \bmod P'$,

$s_{w1} = (x_w)^{\prod_{i=1, w\neq i}^{t}(-v_i)\cdot(v_w - v_i)^{-1}} \cdot (H(M') \cdot (H(M))^{-1})^t \cdot r_{w1} \bmod P'$,

$r_{w2} = g^{k_w} \bmod P$, and

$s_{w2} = k_w^{-1} \cdot (s_{w1} - x_w \cdot r_{w2}) \bmod P'$.

After that, u_w sends $(M, r_{w1}, s_{w1}, r_{w2}, s_{w2})$ to CLK. Note that CLK will accept (s_{w1}, r_{w2}, s_{w2}) as a valid individual signature of M signed by u_w, because it will pass the equality test through Equation 1, and thereby he will combine the forged individual signature (s_{w1}, r_{w2}, s_{w2}) with other $t-1$ valid individual signatures into the construction a group signature (R,S) for M', not the original M. For a later time, u_w could present (M', R, S) to a verifier and claim that (R,S) is a valid group signature for M' with respect to G. In this time, (M', R, S) will pass the equality test through Equation 2. Therefore, the verifier will convince that M' is indeed signed by the participant signers in T on behalf of G, through tracing back the participant signers from the public polynomial $h(y)$.

An insider forgery attack on the Wang-Lin-Chang scheme without MTC – Scenario of this attack is somewhat like that against the scheme with MTC, except that u_w computes

$s_{w1} = (\alpha^{f_w(0)} \cdot \prod_{i=t+1}^{n} \alpha^{\lambda_i}) \cdot (H(M') \cdot (H(M))^{-1})^t \cdot r_{w1} \bmod P'$,

where $\lambda_i = f_i(v_w) \prod_{l=1, w\neq l}^{t} (-v_l) \cdot (v_w - v_l)^{-1} \bmod Q$.

The reader is encouraged to verify that the individual signature (s_{w1}, r_{w2}, s_{w2}) for M can pass the equality test through Equation 1. Consequently, CLK will construct a group signature (R,S) for M by combining the forged individual signature (s_{w1}, r_{w2}, s_{w2}) with all verified individual signatures generated by the other participant signers in T. Again, u_w could present (M', R, S) to a verifier for a later time and it will pass the equality test through Equation 2.

4. CONCLUSIONS

We have demonstrated two scenarios of insider forgery attacks on both the Wang-Lin-Chang schemes, respectively. From the analysis mentioned above, the security flaws in both the Wang-Lin-Chang schemes are caused by the facts: First, (r_{i2}, s_{i2}) is independent on the signing message M, and second, (r_{i2}, s_{i2}) can only be used to verify s_{i1}, not (r_{i1}, s_{i1}). These two facts imply that each individual signature (s_{i1}, r_{i2}, s_{i2}) and (M, R, S) are independent. Improvements of the Wang-Lin-Chang schemes that can eliminate these security flaws are our future works under study.

5. REFERENCES

[1] Y. Desmedt, Society and group oriented cryptography, *Advances in Cryptology – CRYPTO '87*, Springer-Verlag, Berlin, 1988, pp. 120-127.

[2] Y. Desmedt and Y. Frankel, Threshold cryptosystems, *Advances in Cryptology – CRYPTO '89*, Springer-Verlag, Berlin, 1990, pp. 307-315.

[3] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, 1976, pp. 644-654.

[4] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, 1985, pp. 469-472.

[5] C.M. Li, T. Hwang, and N.Y. Lee, Threshold-multisignature schemes where suspected forgery implies tractability of adversarial shareholders, *Advances in Cryptology - EUROCRYPT '94*, Springer-Verlag, Berlin, 1994, pp. 194-204.

[6] Y.M. Tseng and J.K. Jan, Attacks on threshold signature schemes with traceable signers, *Information Processing Letters*, Vol. 71, No. 1, 1999, pp. 1-4.

[7] C.T. Wang, C.H. Lin, and C.C. Chang, Threshold signature schemes with traceable signers in group communications, *Computer Communications*, Vol. 21, No. 8, 1998, pp. 771-776.