Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2004 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-5-2004

The Security Flaw of an Untraceable Signature Scheme

Chinchen Chang

Yafen Chang

The Security Flaw of an Untraceable Signature Scheme

Chinchen Chang, Yafen Chang

Department of Computer Science and Information Engineering, National Chung Cheng University,
Chiayi 621, Taiwan, China
e-mail:{ccc, cyf}@cs.ccu.edu.tw

ABSTRACT

In 2003, Hwang et al. proposed a new blind signature based on the RSA cryptosystem. The Extended Euclidean algorithm is employed in their proposed scheme. They claimed that the proposed scheme was untraceable and it could meet all requirements of a blind signature. However, we find that the signer can still trace the blind signature applicant in some cases. Thus, we present the security flaw of Hwang et al.'s scheme in this paper.

Keywords: blind signature, untraceable, RSA, Extended Euclidean algorithm

1. INTRODUCTION

In 1982, Chaum proposed the concept of blind signature [1]. In blind signature schemes, an applicant can obtain a signature of a message from the signer without revealing the content of the signed message to the signer. Blind signature can be used in many cryptographic applications, such as electronic voting systems and electronic cash payment systems. Thus, how to make the resulting message-signature pair not be able to be linked is an important issue. On the other hand, the personal information should be protected while the resulting message-signature pair is used in any application. As a result, Chaum proposed the first blind signature ensuring the user's private information. With the progressive improvement of the blind signature [2], [4]-[6], the requirements of the blind signature, (1) correctness, (2) blindness, (3) unforgeability, and (4) untraceability, are listed and described as follows:

(1) Correctness: Anyone can check the blind signature of the signed message by using the server's public key.

(2) Blindness: The signer has no idea of the content of the signed message.

(3) Unforgeability: Only the signer can generate the signature. That is, no one can forge a valid signature and can have the forged signature verified successfully.

(4) Untraceability: The signer of the blind signature cannot link the message-signature pair even if the signature has been revealed to be public.

Recently, Hwang et al. [7] proposed a blind signature based on the RSA cryptosystem [9]. It also employs the Extended Euclidean algorithm [8]. They claimed that the proposed scheme is untraceable and meets all requirements of a blind signature mentioned above. And the security of the proposed scheme is based on the difficulties of solving the factoring problem. However, in some cases, the signer can still trace the blind signature applicant. As a result, we present its security flaw in this paper.

The rest of the paper is organized as follows. First, we review Hwang et al.'s untraceable blind signature in Section 2. Then the drawback of Hwang et al.'s scheme is shown in Section 3. Finally, the conclusions are given in Section 4.

2. A REVIEW OF HWANG ET AL.'S UNTRACEABLE BLIND SIGNATURE

In this section, we review Hwang et al.'s proposed untraceable blind signature, which consists of five phases: (1) the initialization phase, (2) the blinding phase, (3) the signing phase, (4) the unblinding phase, and (5) the verification phase. The five phases are presented in Subsections 2.1 to 2.5, respectively.

2.1 The Initialization Phase

In this phase, the signer S makes the essential information public as follows:

Step 1. S randomly selects two large prime numbers p and q and computes $n = p\cdot q$ and $\phi(n) = (p-1)(q-1)$.

Step 2. S chooses two large random numbers e and d, where $\gcd(e, \phi(n)) = 1$, $e\cdot d \bmod \phi(n) = 1$.

Step3. S keeps p, q, and d secret and makes e, n, and H public, where H is a one-way hash function—MD5 and SHA-1 [3] for example.

2.2 The Blinding Phase

Suppose the requester R has a message m and wants m signed without being known by S. R performs the following steps to make m concealed.

Setp 1. R randomly selects two distinct numbers t_1 and t_2.

Step 2. R chooses two random primes a_1 and a_2, where $\gcd(a_1, a_2) = 1$.

Step 3. R computes $s_1 = t_1^{e} \cdot H(m)^{a_1} \bmod n$ and $s_2 = t_2^{e} \cdot H(m)^{a_2} \bmod n$.

Step 4. R sends s_1 and s_2 to S.

2.3 The Signing Phase

After getting s_1 and s_2 from R, S generates the corresponding blind signature of m as follows:
Step 1. S randomly chooses two primes b_1 and b_2, where $\gcd(b_1, b_2) = 1$.
Step 2. S computes $r_1 = s_1^{b_1 d} \bmod n$ and $r_2 = s_2^{b_2 d} \bmod n$.
Step 3. S sends (r_1, r_2, b_1, b_2) to R.

2.4 The Unblinding Phase

Upon receiving (r_1, r_2, b_1, b_2), R performs as follows to derive the blind signature s of m.
Step 1. R computes $g_1 = r_1 \cdot t_1^{-b_1} \bmod n$ and $g_2 = r_2 \cdot t_2^{-b_2} \bmod n$.
Step 2. R finds w and t according to Extended Euclidean Algorithm [3], where $(a_1b_1)w + (a_2b_2)t = 1$, and keeps b_1, b_2, w, and t secret.
Step 3. R computes $s = g_1^w \cdot g_2^t \bmod n$ and then publishes (m, s).

2.5 The Verification Phase

In order to verify the signature s of m, the verifier V computes H(m) and $s^e \bmod n$. Then V checks whether $H(m) = s^e \bmod n$ holds or not. If it holds, it denotes that s is indeed the signature of m.

3. THE SECURITY FLAW OF HWANG ET AL.'S UNTRACEABLE BLIND SIGNATURE

In this section, we are going to show how the signer traces the blind signature in Hwang et al.'s proposed scheme. To make tracing the blind signature easier, S chooses two primes p and q, where $4|p+1$ and $4|q+1$, and computes $n = p \cdot q$ and $\phi(n) = (p-1)*(q-1)$. Then S randomly chooses two large numbers e and d, where $\gcd(e, \phi(n)) = 1$, $e \cdot d \bmod \phi(n) = 1$.

First, as shown in the blinding phase, R has a message m and wants m signed without being known by S. Then, R performs as follows:
Setp 1. R randomly selects two distinct numbers t_1 and t_2.
Step 2. R chooses two random primes a_1 and a_2, where $\gcd(a_1, a_2) = 1$.
Step 3. R computes $s_1 = t_1^e \cdot H(m)^{a_1} \bmod n$ and $s_2 = t_2^e \cdot H(m)^{a_2} \bmod n$.
Step 4. R sends s_1 and s_2 to S.

Second, as shown in the signing phase, S generates the corresponding blind signature of m as follows:
Step 1. S chooses two random primes b_1 and b_2, where $\gcd(b_1, b_2) = 1$.
Step 2. S computes $r_1 = s_1^{b_1 d} \bmod n$ and $r_2 = s_2^{b_2 d} \bmod n$.
Step 3. S sends (r_1, r_2, b_1, b_2) to R.

Third, as shown in the unblinding phase, R gets (m, s), where $s = H(m)^d \bmod n$. After performing the above procedures several times, S can get (s_1, s_2)'s and ($s_1^d \bmod n$, $s_2^d \bmod n$)'s. Because $s_1 = t_1^e \cdot H(m)^{a_1} \bmod n$ and $s_2 = t_2^e \cdot H(m)^{a_2} \bmod n$, we can have $s_1^d = t_1 * (H(m)^d)^{a_1} \bmod n$ and $s_2^d = t_2 * (H(m)^d)^{a_2} \bmod n$. That is, S can collect all the ($t_1 * (H(m)^d)^{a_1} \bmod n$, $t_2 * (H(m)^d)^{a_2} \bmod n$)'s.

Now, suppose that S knows (m', δ), where $\delta = H(m')^d \bmod n$. If t_1, t_2, and ($H(m)^d \bmod n$) are co-prime and $a_1 < a_2$ possibly, S can find the relation between ($s_1^d \bmod n$, $s_2^d \bmod n$) and δ as follows:
Step 1. S computes $\gcd(t_1 * (H(m)^d)^{a_1} \bmod n,\ t_2 * (H(m)^d)^{a_2} \bmod n) = H(m)^{d*a_1} \bmod n$.
Step 2. S computes $\eta = (H(m)^{d*a_1} \bmod n) * \delta \bmod n$.
Step 3. S computes
$c_1 = \eta^{(p+1)/4} \bmod p$,
$c_2 = (p - \eta^{(p+1)/4}) \bmod p$,
$c_3 = \eta^{(q+1)/4} \bmod q$,
$c_4 = (q- \eta^{(q+1)/4}) \bmod q$,
$x = q(q^{-1} \bmod p)$, $y = p(p^{-1} \bmod q)$,
$\beta_1 = (xc_1+yc_3) \bmod n$,
$\beta_2 = (xc_1+yc_4) \bmod n$,
$\beta_3 = (xc_2+yc_3) \bmod n$, and
$\beta_4 = (xc_2+yc_4) \bmod n$ [8].
Step 4. If there exists a β_j such that $\beta_i * \delta^{(\phi(n)/2)} = \beta_j \bmod n$, where $i \neq j$ and $1 \leq i, j \leq 4$, this denotes that δ is related to ($t_1 * (H(m)^d)^{a_1} \bmod n$, $t_2 * (H(m)^d)^{a_2} \bmod n$).
If m=m′, we have

$$\eta = (H(m)^d)^{a_1+1} \bmod n . \qquad (1)$$

Because a_1 is odd, a_1+1 is an even number. As a result,

$$\eta = ((H(m)^d)^{(a_1+1)/2})^2 \bmod n . \qquad (2)$$

Equation (2) can be rewritten as the follow equation.

$$\eta = (((H(m)^d)^{(a_1+1)/2})^2 \bmod n) * (H(m)^{\phi(n)} \bmod n) \bmod n. \qquad (3)$$

Since m = m′, we have

$$\eta = (((H(m)^d)^{(a_1+1)/2})^2 \bmod n) * (H(m')^{\phi(n)} \bmod n) \bmod n \qquad (4)$$

$$= (((H(m)^d)^{(a_1+1)/2} \bmod n) * (H(m')^{\phi(n)/2} \bmod n))^2 \bmod n. \qquad (5)$$

According to the above equation, we can get

$$\eta^{1/2} = ((H(m)^d)^{(a_1+1)/2} \bmod n) * (H(m')^{\phi(n)/2} \bmod n) \bmod n. \qquad (6)$$

From Equation (1), we have

$$\eta^{1/2} = ((H(m)^d)^{(a_1+1)/2} \bmod n) . \qquad (7)$$

According to the properties of Rabin's [8], we know there exist at most four distinct solutions for $\eta^{1/2}$ mod n. That is, at least one β_i will equal to $((H(m)^d)^{(a_1+1)/2} \bmod n)$ for $1 \le i \le 4$. Therefore, if m = m′, we have

$$\beta_j = \beta_i * (H(m')^{\phi(n)/2} \bmod n) \bmod n \quad (8)$$
$$= \beta_i * \delta^{\phi(n)/2} \bmod n. \quad (9)$$

As a result, S checks whether any $\beta_i * \delta^{(\phi(n)/2)} = \beta_j \bmod n$ for $1 \le i, j \le 4$ and $i \ne j$, in Step 4.

According to the above procedures, it is obvious that S can trace the blind signature in Hwang et al.’s proposed blind signature scheme.

4. CONCLUSIONS

Hwang et al. proposed a new blind signature based on the RSA cryptosystem by employing the Extended Euclidean algorithm. Though they claimed that the proposed scheme was untraceable and it could meet all requirements of a blind signature, however, we find that the signer can still trace the blind signature applicant in some cases. On the other hand, the computation load of Hwang et al’s scheme is too heavy. There still exists space for improving the proposed blind signature scheme.

REFERENCES

[1] Chaum, D., “Blind Signatures for Untraceable Payments,” Proceedings of Advances in Cryptology Crypto’82, Santa Barbara, California, USA, pp. 199-203, 1982.

[2] Chaum, D., “Blinding Signatures System,” Proceedings of Advances in Cryptology Crypto’83, Santa Barbara, California, USA, pp. 153-156, 1983.

[3] Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A., Handbook of Applied Cryptography, CRC Press, 1996.

[4] Fan, C.-I. Chen, W.-K., and Yeh, Y.-S., “Randomization Enhanced Chaum’s Blind Signature Scheme,” Commuter Communications, Vol. 23, pp. 1677-1680, 2000.

[5] Juang, W.-S. and Lei, C.-L., “Partially Blind Threshold Signatures Based on Discrete Logarithm,” Computer Communications, Vol. 22, pp. 73-86, January 1999.

[6] Shao, Z., “Improved User Efficient Blind Signature,” Electronics Letters, Vol. 36, No. 16, pp. 1372-1374, 2000.

[7] Hwang, M.-S., Lee, C.-C., and Lai, Y.-C., “An Untraceable Blind Signature Scheme,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E86-A, No. 7, pp. 1902-1906, July 2003.

[8] D. Kahn, The Codebreakers: The Story of Secret Writing, Macmillan Publishing Co., New York, 1967.

[9] Chang, C.-C. and Hwang, M.-S., “Parallel Computation of the Generating Keys for RSA Cryptosystems,” IEE Electronics Letters, Vol. 32, No. 15, pp. 1365-1366, 1996.