Cryptanalysis of Sun et al.’s Directed Digital Signature Scheme

Eun-Jun Yoon

Department of Cyber Security, Kyungil University
33 Buho-Ri, Hayang-Ub, Kyungsan-Si
Kyungsangpuk-Do 712-701, Republic of Korea

Copyright © 2015 Eun-Jun Yoon. This article is distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract
In 2015, Sun et al. proposed an improved directed digital signature scheme using a non-interactive public-key distribution system. Sun et al. claimed that their proposed directed digital signature scheme is secure to message forgery attacks. However, this paper points out that Sun et al.’s scheme is still vulnerable to message forgery attacks unlike their claims. For this reason, Sun et al.’s scheme is insecure for practical application.

Keywords: Cryptography; Digital signature; Non-interactive; Public-key distribution; Cryptanalysis; Message forgery attack

1 Introduction

In 1991, Maurer and Yacobi[1] proposed an identity-based non-interactive public-key distribution system based on a novel trapdoor one-way hash function of exponentiation modulo of a composite number. In 1998, Tseng et al.[2] improved the squaring method based on the Maurer and Yacobi scheme and then proposed a directed digital signature scheme, a user identification scheme, and a conference key distribution system[3, 4].

However, in 2015, Sun et al.[5] proved that Tseng et al.’s scheme cannot prevent a forgery attack. It means that any user can easily forge a signature to get any message successfully and then declare that it is generated by

1Corresponding author. Tel.: +82-53-600-5623; Fax: +82-53-600-5639
other users in the Tseng et al.’s scheme. Moreover, Sun et al. proposed an improved directed digital signature scheme using a non-interactive public-key distribution system. Sun et al. claimed that their proposed directed digital signature scheme is secure to message forgery attacks. However, this paper points out that Sun et al.’s scheme is still vulnerable to message forgery attacks unlike their claims. For this reason, Sun et al.’s scheme is insecure for practical application.

This paper is organized as follows: Section 2 briefly reviews the Sun et al.’s directed digital signature scheme. The security flaws of Sun et al.’s scheme are shown in Section 3. Finally, conclusions are given in Section 4.

2 Review of Sun et al.’s Directed Digital Signature Scheme

This section briefly reviews Sun et al.’s directed digital signature scheme[5]. Fig. 1 depicts the Sun et al.’s scheme. There are three phases in the Sun et al.’s scheme: the system initialization phase, the user registration phase, and the directed digital signature phase. The three phases are described as follows:

2.1 System Initialization Phase

The trusted authority generates system parameters as follows:

1. \( N \) denotes the product of four primes \( p_j \) which are between 60 and 70 decimal digits, where the numbers \((p_j - 1)/2\) are odd and pair-wise relatively prime.

2. \( e \) denotes an integer in \( \mathbb{Z}^*_{\varphi(N)} \) and the secret value \( d \) is satisfied by the equation \( e \cdot d \equiv 1(\text{mod} \varphi(N)) \), where \( \varphi \) is the Euler’s totient function.

2.2 User Registration Phase

Suppose that a user \( U_A \) wants to join the system presents with his/her unique identity \( ID_A \). The user registration phase performs as follows:

1. The trusted authority randomly chooses a secret number \( t \) from \( \mathbb{Z}^*_{\varphi(N)} \).

2. The trusted authority computes \( s_A \) for \( U_A \) in secret as follows:

\[
s_A \equiv e \cdot t \cdot \log_g(ID_A^2)(\text{mod} \varphi(N)) \quad (1)
\]

where \( g \) is a primitive element in \( GF(p_j) \).
3. The trusted authority computes

$$v \equiv t^{-1}(\text{mod} \varphi(N))$$

(2)

4. The trusted authority publishes \(\{N, g, e, h(\cdot)\}\) and keeps \(\{p_1, p_2, p_3, p_4, t, v, d\}\) secret, where \(h(\cdot)\) is a secure one-way function.

5. The legal user \(U_A\) publishes \(ID_A\) and keeps \(s_A\) secret.

### 2.3 Directed Digital Signature Phase

Assume the legal user \(U_A\) wants to sign a message \(M\) and send it to the specific receiver \(U_B\). The signature generation procedure performs as follows:

1. \(U_A\) chooses a random integer \(k\) in \(\mathbb{Z}_N^*\) and computes the signature \((r, s)\) for message \(M\) as follows:

$$r = g^k(\text{mod} N)$$

(3)

$$s = (ID_B^2)^{s_A \cdot h(M,r)} \cdot g^{d-k}(\text{mod} N)$$

(4)

2. \(U_A\) sends \((M, r, s)\) to \(U_B\).

3. Upon receiving \((M, r, s)\), \(U_B\) can verify the signature of the message \(M\) by the following equation:

$$s^e \equiv (ID_A^2)^{e \cdot s_B \cdot h(M,r)} \cdot r(\text{mod} N)$$

(5)

4. If the above verified equation holds, the signature for message \(M\) by \(U_A\) is verified. The specific verifier only verifies the validity of the signature for message \(M\) by the unique identity of the signer.

### 3 Message Forgery Attack on Sun et al.’s Directed Digital Signature Scheme

This section demonstrates that Sun et al.’s directed digital signature scheme[5] cannot withstand a message forgery attack.

Assume the sender \(U_A\) generates the signature \((r, s)\) for the message \(M\) and then sends it to a specified receiver \(U_B\). In general, the value \(\{M, r, s\}\) are only generated by the sender \(U_A\). However, in the Sun et al.’s scheme, the receiver
Choose $k \in \mathbb{Z}_N^*$.

\[ r = g^k \pmod{N} \]
\[ s = (ID_B^2)^{s_A \cdot h(M,r)} \cdot g^{sk} \pmod{N} \]

\[ \{M, r, s\} \]

Verify $s^e \equiv (ID_A^2)^{s_B \cdot h(M',r')} \cdot r' \pmod{N}$

$U_B$ can easily forge the signature $(r', s')$ for the message $M'$ and then declare that the signature $(r', s')$ is generated by the sender $U_A$.

For example, the receiver $U_B$ can easily forge the signature $(r', s')$ for the message $M'$ as follows:

1. $U_B$ chooses a random integer $k' \in \mathbb{Z}_N^*$.

2. $U_B$ computes the forged signature $(r', s')$ for message $M'$ as follows:

\[ r' = g^{e \cdot k'} \pmod{N} \tag{6} \]
\[ s' = (ID_B^2)^{s_B \cdot h(M',r')} \cdot g^{k'} \pmod{N} \tag{7} \]

3. $U_B$ finally sends the forged signature $(r', s')$ for message $M'$ to a specified receiver.

4. Upon receiving $(M', r', s')$, the specified receiver will verify the signature of the message $M'$ by the following equation:

\[ (s')^e \equiv (ID_A^2)^{e \cdot s_B \cdot h(M',r')} \cdot r' \pmod{N} \tag{8} \]

Because the above verified equation always holds, the forged signature $(r', s')$ for message $M'$ by the user $U_B$ is also verified correctly.

The forged signature $(r', s')$ for message $M'$ is verified correctly as follows:
Therefore, $U_B$ can forge the signature for any message and then declare that the signature is generated by $U_A$. In other words, the user can easily forge the signature and then declare that it is generated by the other user. The problem is that any user $U_A$ or $U_B$ can easily compute $(ID_A^2)^{s_B \cdot e}$ and $(ID_B^2)^{s_A \cdot e}$ respectively by the following equation:

\[(ID_A^2)^{s_B \cdot e} = g^{d \cdot s_A \cdot s_B \cdot e} = (ID_B^2)^{s_A \cdot e}\]  (10)

Therefore, Sun et al.’s scheme is still vulnerable to the above message forgery attack unlike their claims.

4 Conclusions

This paper reviewed Sun et al.’s directed digital signature scheme and then pointed out that the scheme is still vulnerable to message forgery attacks unlike their claims. Consequently, Sun et al.’s scheme is insecure for practical application. Further works will be focused on improving Sun et al.’s scheme which can be able to provide greater security and to be more efficient than the existing digital signature schemes by an accurate performance analysis.

Acknowledgements. This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP)(No. 2015R1A2A2A01006824) and partially supported by Small & Medium Business Administration grant funded by the Korea government(SMBA)(No. C0332654).

References


Received: October 21, 2015; Published: December 12, 2015