Comments: cryptanalysis of Tseng et al.'s authenticated encryption schemes

Yi-Hwa Chen and Jinn-Ke Jan*

Institute of Applied Mathematics, National Chung Hsing University

Taichung Taiwan 402, R.O.C, E-mail: yh_chen@seed.net.tw

*Institute of Computer Science, National Chung Hsing University

Taichung Taiwan 402, R.O.C, E-mail: jkjan@cs.nchu.edu

Abstract

Digital signatures are important because they provide not only end-to-end message integrity guarantees but also authentication information about the originator of a message. In Recently, Xie and Yu proposed a forgery attack on the Tseng et al's authenticated encryption schemes and showed that their schemes are not secure in two cases: the specified verifier substitutes his secret key, or the signer generates the signature with these schemes for two or more specified verifiers. In addition, Xie and Yu made a small modification for the Tseng et al's schemes and claimed that the modified schemes can satisfy the security requirement. However, we show that the modified schemes are still insecure.

Keywords: *Cryptography; Authenticated encryption; Message linkage; Self-certificated public key*

1. Introduction

Digital signature is one of the most important techniques in the modern electronic environments, especially used in e.g. e-commerce etc. The signer generates a signature for a given message with his secret key, the verifier verifies if the signature is valid or not with the signer's public key. Based on the discrete logarithm problem, Nyberg and Rueppel [1] proposed the signature scheme with the property of message recovery. A concern point for the message recovery is that let the specified verifier be able to verify and recover the message but prevent from the others doing that. To achieve this purpose, a signature signed by the signer must be encrypted with the verifier's public key. It is natural but inefficient by the reason of a lot of overload on computation and data communications. Therefore, Horster et al. [2] and

other researchers [3-5] proposed the authenticated encryption schemes to improve the efficiency.

In 2003, Tseng et al. [6] first proposed a new type signature scheme with message recovery by using the technique of self-certified public keys. Their scheme provides two properties: (1) the signer's public key can simultaneously be authenticated in verifying the signature, and (2) the receiver obtains the message at the same time. In their scheme, certificate directory with the user's public key maintained in the system authority is not necessary. Therefore, Tseng et al's scheme reduces the necessary message space of system authority and communication costs of the verifier.

Recently, Xie and Yu [7] found that Tseng et al's scheme is insecure against the forgery attack. By substituting the specified verifier's secret key or cooperating with a new user who uses the special deduced secret key to joint the system, the specified verifier and his cooperator can forge the valid signature for any message. In addition, Xie and Yu made a modification on Tseng et al's scheme to overcome this weakness.

In this paper, we will show that Xie and Yu's modified scheme is still vulnerable to the forgery attack.

2. Xie and Yu's modified scheme

In this section, we first review Xie and Yu's modified scheme. Their scheme is composed of three phases: the system initialization phase, signature generation phase, and message recovery phase.

In the initialization phase, a trusted center selects the system parameters as follows: Let p and q be prime numbers such that $p = 2p^* + 1$ and $q = 2q^* + 1$, where p^* and q^* are also primes. Then, computes $N = pq$, let g be a generator of a multiplicative subgroup with order p^*q^*, $h(.)$ denotes a one-way collision resistant hash function. The trusted center publishes N, g, and $h(.)$ to all users and keeps p, q, p^* and q^* secret.

A user U with identity ID_U randomly chooses a secret key x_U and computes $P_U = g^{x_U} \bmod N$. Then, U sends ID_U, P_U to the trusted center and obtains its corresponding public key y_U from the trusted center, where

$$y_U = (P_U - ID_U)^{h(ID_U)^{-1}}.$$

In the signature generation phase, a signer U_S wants to generate a signature blocks of the large message M for a specified verifier U_V. Message M is embedded with some redundancy against forgery attack and is separated into k pieces of $\{M_1, M_2, ..., M_n\}$, where $M_i \in GF(N)$ for $i = 1,2,...,n$. The signer U_S performs the following steps to generate the signature:

1. Choose a random number k and compute $t = (y_V^{h(ID_V)} + ID_V)^k \bmod N$.
2. Let $r_0 = 0$ and compute $r_i = M_i h(r_{i-1} \oplus t) \bmod N$ for $i = 1,2,...,n$, where "$\oplus$" denotes the concatenation operator.
3. Compute $r = h(r_1 \| r_2 \| ... \| r_n)$, where "$\|$" denotes the concatenation operator, and $s = k - x_S r$.
4. Send $n+3$ signature blocks $(r, s, g^k, r_1, r_2, ..., r_n)$ to U_V.

In the message recovery phase, upon receiving the signature blocks from U_S, U_V works as follows:

1. Compute $g^{k^*} = g^s (y_S^{h(ID_S)} + ID_S)^r \bmod N$ and check if $g^k = g^{k^*}$ holds or not.
2. Compute $r^* = h(r_1 \| r_2 \| ... \| r_n)$ and check if $r = r^*$ holds or not.
3. Compute $t = g^{kx_V} \bmod N$.
4. Recovery the message blocks $\{M_1, M_2, ..., M_n\}$ as follows:

   $M_i = r_i h(r_{i-1} \oplus t)^{-1} \bmod N$.

3. Security Analysis

Xie and Yu proposed a successful attack to the Tseng et al's authenticated encryption scheme. To overcome this weakness, Xie and Yu made a small modification on Tseng et al's scheme. However, in this section, we will show that the modified scheme is still insecure against the forgery attack. The detailed procedure is described as follows:

3.1 Forgery attack

The specified verifier U_V has ever recovered the message blocks $\{M_1, M_2, ..., M_n\}$ from a signature $(r, s, g^k, r_1, r_2, ..., r_n)$ received from the signer U_S and tries to forge a valid signature $(r', s', g^{k'}, r_1', r_2', ..., r_n')$ for message $\{M_1', M_2', ..., M_n'\}$. The verifier U_V performs the following steps:

1. Compute $t = (g^k)^{x_V} \bmod N$.
2. Let $r_0' = 0$ and compute $r_i' = M_i' h(r_{i-1}' \oplus t) \bmod N$ for $i = 1,2,...,n$.
3. Compute $r' = h(r_1' \| r_2' \| ... \| r_n')$.
4. Compute $x_V' = r x_V (r')^{-1}$ and $s' = s x_V (x_V')^{-1}$.
5. Compute $g^{k'} = g^{s'} (y_S^{h(ID_S)} + ID_S)^{r'} \bmod N$.

The specified verifier U_V may replace the original secret key x_V with x_V' to trusted center, then the U_V can forge the signature for any message, or the U_V provides the secret key x_V' to a new user U_U to joint the system, then they can forge the signature for any messages by cooperating each other.

3.2 Correctness

The method of the forgery attack is to fix the value of t such that the following deduction holds

$$t = g^{k' x_V'} = [g^{s'} (y_S^{h(ID_S)} + ID_S)^{r'}]^{x_V'} = [g^{s'} g^{x_S r'}]^{x_V'} = g^{s' x_V' + x_S r' x_V'} = g^{s x_V + x_S r x_V} = g^{(s + x_S r) x_V}$$

$$= g^{k x_V} \bmod N$$

So without knowing the value of k, the specified verifier or verifiers still can forge any valid signature by computing $g^{k'}$. Therefore, Xie and Yu's modified schemes are still insecure.

4. Conclusion

Tseng et al. proposed a new type signature scheme with message linkage for message blocks, which could prevent the signature blocks from being reordered, replicated, or partially deleted during the transmission. Xie and Yu proposed a forgery attack on the Tseng et al.'s schemes

and furthermore made a modification to mend its weakness. However, this paper points out that Xie and Yu's modified scheme is not secure either.

References

[1] K. Nyberg, R.A. Rueppel, Message recovery for signature schemes based on the discrete logarithm, Designs, Codes Cryptography 7 (1996) 61-81.

[2] P. Horster, M. Michels, H. Peterson, Authenticated encryption scheme with low communication costs, Electronics Letters 30 (15) (1994) 1212.

[3] Y.M. Tseng, J.K. Jan, An efficient authenticated encryption scheme with message linkages and low communication costs, J. Inform. Sci. Engrg. 18 (1) (2002) 41-46.

[4] Y.M. Tseng, J.K. Jan, H.Y. Chien, Authenticated encryption scheme with message linkages for message flows, Computers and Electrical Engineering, accepted and to appear.

[5] T.S. Wu, C.L. Hsu, Convertible authenticated encryption scheme, The Journal of System and Software 62 (2002) 205-209.

[6] Y.M. Tseng, J.K. Jan, H.Y. Chien, Digital signature with message recovery using self-certified public keys and its variants, Applied Mathematics and Computation 136 (2003) 203-214.

[7] Q. Xie, X.Y. YU, Cryptanalysis of Tseng et al.'s authenticated encryption schemes, Applied Mathematics and Computation 158 (2004) 1-5.