Cryptanalysis of improvement of digital signature with message recovery using self-certified public keys and its variants

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

In 2003, Tseng et al. proposed a self-certified public key signature with message recovery, which gives two advantages: one is that the signer's public key can simultaneously be authenticated in verifying the signature and the other one is that only the specified verifier can recover the message. Lately, Xie and YU proposed an attack to the Tseng et al.'s scheme under the cases: the specified verifier substitutes his secret key or two or more specified verifiers cooperatively forge the signer's signature. About the same time, Shao also proposed another insider forgery attack to break the Tseng et al.'s scheme. In addition, he claimed the Tseng et al.'s scheme without the properties of non-repudiation and forward security. Therefore, he proposed an improved scheme to overcome the weakness. In this paper, we will show that the Shao's improved scheme is still insecure against the insider forgery attack. A specified verifier can forge many different valid signatures with the same message to the other verifiers who cooperatively provide their secret keys. Furthermore, we give a small modification to overcome this weakness.

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

1. Introduction

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 applications, they are suitable for using in electronic commerce, electronic voting, and so on.

Usually, the signer first generates a signature for a given message with his secret key, the verifier then verifies whether the signature is valid or not with the signer's public key. However, verifying a signature can be divided into two catalogues: one is that the signature is verified with clear message and the other one is that the signature is verified with message recovery. The former means that anyone can verify the signature since which message is clear. However, a concern point for the latter is that only the specified verifier is able to verify and recover the message but prevent from the others doing that. Based on the discrete logarithm problem, Nyberg and Rueppel [1] proposed the signature scheme with the property of message recovery. To achieve this purpose of message recovery, a signature must be signed by the signer before it is encrypted with the verifier's public key. The process 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] proposed a new type signature scheme with message recovery by using the technique of self-certified public keys. They also presented two variants based on the proposed scheme. One is an authenticated encryption scheme used for short message and the other one is an authenticated encryption scheme, with message linkages, used for large message. Their schemes provide 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 schemes, certificate directory with the user's public key maintained in the system authority is not necessary. Therefore, Tseng et al's schemes reduce 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. About the same time, Shao [8] also proposed another insider forgery attack to break the Tseng et al.'s schemes. He assumed that an dishonest system authority maybe cooperate with a third party A to set up a legitimate user B in the system by forging a valid signature and claim that the forged signature is signed by B to A. In addition, Shao claimed the Tseng et al.'s schemes without the properties of non-repudiation and forward security. Therefore, he proposed an improved scheme to overcome the weakness.

In this paper, we will show that Shao's improved scheme is still vulnerable to the insider forgery attack such that we make a small modification to mend this weakness. In section 2, a brief review of the Shao's improved scheme is presented. Section 3 discusses the security of the Shao's improved scheme and proposes a small modification. Finally, a conclusion is given.

2. Shao's improved scheme

In this section, we will review the Shao's improved authenticated encryption scheme with message linkages using for large message. Their scheme is composed of four phases: the system initialization phase, signature generation phase, message recovery phase and dispute arbitration phase.

System initialization phase: A trusted authority (TA) 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, TA computes $N = pq$ and let g be a generator of a multiplicative subgroup with order $p^* q^*$. Symbol $h(\ )$ denotes a one-way collision resistant hash function. Finally, TA 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 TA and obtains its corresponding public key y_U from the TA, where $y_U = (P_U - ID_U)^{h(ID_U)^{-1}}$.

Signature generation phase: Assume that a signer U_S wants to sign and encrypt a signature blocks of the large message M to a specified verifier U_V. Message M is embedded with some redundancy against forgery attack and is made of the sequence of $\{M_1, M_2, ..., M_n\}$, where $M_i \in GF(N)$ for $i = 1,2,...,n$. That also means $M = M_1 \| M_2 \| ... \| M_n$, where '||' denotes the concatenation operator. The signer U_S performs the following steps to generate the signature:

1. Choose a random number k to compute $t = (y_V^{h(ID_V)} + ID_V)^k \bmod N$ and $e = g^k \bmod N$.
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 exclusive-or operator.
3. Compute $r = h(M, e)$ and $s = k - x_S r$.
4. Send $n+2$ signature blocks $(r, s, r_1, r_2, ..., r_n)$ to U_V.

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 then compute $t = (g^k)^{x_V} \bmod N$ with his private key x_V.

2. Set $r_0 = 0$ and recovery the message blocks $\{M_1, M_2, ..., M_n\}$ as follows:

$$M_i = r_i h(r_{i-1} \oplus t)^{-1} \bmod N \text{ for } i = 1, 2, ..., n.$$

3. Verify the signature by checking if the equation $r = h(M, g^s \cdot (y_V^{h(ID_V)} + ID_V)^r \bmod N)$ holds.

Dispute arbitration phase: The phase only operates in the situation when there are some disputes over the message signed, the signer or the verifier should provide the message M to the verification equation in order to convince a third party if the signature is valid. Without the message M, any third party cannot arbitrate the message signed to be valid or not. Upon obtaining M, the third party verifies the signature with the following verification equation:

$$r = h(M, g^s \cdot (y_V^{h(ID_V)} + ID_V)^r \bmod N)$$

3. Security Analysis

Shao claimed that his improved scheme could prevent against the insider forgery attack. However, in this section, we will show that his improved scheme is still insecure against the insider forgery attack. A specified verifier U_V owning a valid message signed can forge many different valid signatures with the same message owned to the other verifiers if they are willing to provide their secret keys to U_V. Think about the condition: a group of people wants to see the game of football, however, only one person actually buys an electronic ticket and then he can forge a number of valid electronic tickets to another persons in the group. Obviously, the attack may cause a lot of losses in the applications of business and result in important leaks of security of the system. Furthermore, when the system using in a sensitive environment, the attack may cause more serious influence, e.g. forgery of e-ticket in election, or forgery of e-cash in e-commerce. The detailed procedure is described as follows:

3.1 Insider forgery attack

The specified verifier U_V has ever recovered the message blocks $\{M_1, M_2, ..., M_n\}$ from a signature $(r, s, r_1, r_2, ..., r_n)$ signed by the signer U_S and tries to forge a valid signature $(r, s, r_1^{'}, r_2^{'}, ..., r_n^{'})$ for the same message to another verifier U_O. The forged signature $(r, s, r_1^{'}, r_2^{'}, ..., r_n^{'})$ presents a valid signature signed by the signer U_S to the verifier U_O. The verifier U_O first provides his secret key x_O to the verifier U_V, U_V then performs the insider forgery attack by the following steps:

1. Compute $g^k = g^s (y_S^{h(ID_S)} + ID_S)^r \bmod N$.
2. Compute $t^{'} = (g^k)^{x_O} \bmod N$.

3. Let $r_0^{'}=0$ and compute $r_i^{'}=M_i h(r_{i-1}^{'}\oplus t^{'})\bmod N$ for $i=1,2,...,n$.
4. Generate a valid signature $(r,s,r_1^{'},r_2^{'},...,r_n^{'})$ to the verifier U_O.

The verifier U_O must trust the specified verifier U_V such that he is willing to reveal his secret key to U_V. Otherwise, the specified verifier U_V can introduce a new user who trusts him to joint the system then they can forge the signatures for the messages known by cooperating each other.

3.2 Correctness

The forged signature is $(r,s,r_1^{'},r_2^{'},...,r_n^{'})$and the original signature is $(r,s,r_1,r_2,...,r_n)$, both of them are signed for the same message M, where$M=M_1\|M_2\|...\|M_n$. The verification equation in the message recovery phase or dispute arbitration phase is $r=h(M,g^s\cdot(y_V^{h(ID_V)}+ID_V)^r\bmod N)$. The verification equation will hold since the forged signature with the same (r,s,M) as the original signature. The weak point in Shao's improved scheme is that the verification equation cannot find the change even the $(r_1,r_2,...,r_n)$ of the original signature has replaced with the values of $(r_1^{'},r_2^{'},...,r_n^{'})$.

3.3. A small modification

In this section, we provide a small modification to overcome the weak point of the Shao's improved scheme. The system initialization phase is the same as the Shao's improved scheme. In signature generation phase, we only change the equation $r=h(M,e)$into $r=h(M^*,e)$, where $M^*=M_1\|M_2\|...\|M_n\|r_1\|r_2\|...\|r_n$. In message recovery and dispute arbitration phase, the corresponding verification equation is changed into $r=h(M^*,g^s\cdot(y_V^{h(ID_V)}+ID_V)^r\bmod N)$.

The small modification provides four properties as follows.

1. Even though the length of M^* becomes longer, the signature remains the same length as the Shao's improved scheme. The reason is that the r in the signature is deduced from M^* and e being hashed and thus its length is still unchanged.
2. Compared with the Shao's improved scheme, only one more concatenation operation is required in the modification. IF the message M^* is viewed as a value with longer length, then the computation time of the concatenating operation seems to be negligible. Therefore, the modified scheme seems to be with the same efficiency as the original one.
3. Changing the value of M_i or r_i, $i=1,2,...,n$, will result in the change of the value of M^*. Therefore, adversary must change the values of r,s in the signature to make the verification

equation $r = h(M^*, g^s \cdot (y_V^{h(ID_V)} + ID_V)^r \bmod N)$ hold. However, he will face the difficulty of computing discrete logarithm [9,10] and factorization problems [11].

4. Only changing the form from message M to M^* in verification equation, the insider forgery attack proposed in section 3.1 no more succeeds by the reason of description in 3 above. Therefore, the modified scheme preserves the main merits inherent in the self-certified public key cryptographic system.

4. Conclusion

We have showed that Shao's improved scheme is vulnerable to the insider forgery attack. A specified verifier U_V owning a valid message signed can forge many different valid signatures with the same message owned to the other verifiers if they are willing to provide their secret keys to U_V. In modern electronic environments, this attack may cause an important disaster especially when the system is used in e.g. e-voting in election or e-payment in e-commerce. A small modification for the Shao's improved scheme is given to overcome the above-mentioned weakness.

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.

[8] Z. Shao, Improvement of digital signature with message recovery using self-certified public keys and its variants, Applied Mathematics and Computation 159 (2004) 391-399.

[9] W. Diffee, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (6) (1976) 644-654.

[10] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory 31 (4) (1985) 469-472.

[11] R.L. Rivest, A. Shamir, L. Adelman, A method for obtaining digital signature and public key cryptosystem, Comm. ACM 21 (2) (1978) 120-126.