International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Security Analysis of Digital Signature Scheme with Message Recovery using Self-Certified Public Keys

Mahshid Sadeghpour*

Iran University of Science and Technology, Tehran, Iran
Email: sadeghpour.mahshid@gmail.com

Abstract

Tseng and his colleagues have proposed two variants of authenticated encryption scheme using self-certified public keys. Their schemes have two fundamental properties. Only the intended receiver can recover the message while verifying the signature, and each user can use his own private key independently without system authority learning about it. This paper presents man-in-the-middle attacks to both Tseng and his colleagues authenticated encryption variants. It will be shown that these schemes are not secure against this attack.

Keywords: Self-certified public key; Authenticated encryption; Digital signature; Man-in-the-middle attack.

1. Introduction

Digital signature plays a key role in modern cryptographic communications. It not only provides authenticity and integrity, but also digital signature brings non-repudiation with it. Like ElGamal digital signature scheme [2], the basic digital signature sends the message via its signature as an appendix, and like Tseng and his colleagues authenticated encryption scheme [11], the digital signature with message recovery encrypts the message in the signature.

In 1991, Girault [4] introduced a novel public key cryptosystem called self-certified public key. In this cryptosystem every user is able to choose his own private key. This means that in self-certified public key cryptosystems each user's public key is generated by a system, while the private key is only known by the user himself. Three years later, in1994, Nyberg and Rueppel [7] introduced a digital signature scheme with message recovery based on discrete logarithm problem. The digital signature scheme with message recovery is a digital signature scheme in which the message is embedded in the signature and the verifier is able to recover the message as he verifies the signature.

---

* Corresponding author.

In 1994, Horster and his colleagues [5] presented a modification to Nyberg and Rueppel's scheme. In their modified scheme, only the specified receiver could verify and recover the intended message. Based on the three schemes mentioned above, in 2003, Tseng and his colleagues [11] proposed two variants of self-certified authenticated encryption schemes: 1) The authenticated encryption scheme, 2) The authenticated encryption scheme with message linkages. The authenticated encryption scheme is the integration of digital signature and encryption scheme. In the authenticated encryption scheme, only the specified receiver can verify and recover the embedded message. It can provide authenticity, privacy and integrity in a smaller bandwidth since the intended message would not be sent by the digital signature as an appendix. The authenticated encryption scheme with message linkages is applicable for large messages. In the authenticated encryption scheme with message linkages, each message M must be divided into a sequence of smaller messages like $\{M_1, \dots, M_n\}$. The scheme helps linking the message blocks to prevent messages being reordered, partially deleted, or replicated during transmissions. In 2004, Xie and his colleagues [12] claimed that Tseng and his colleagues authenticated encryption scheme with message linkages is insecure against forgery attack. They provided a forgery attack based on the substitution of specified receiver's secret key. They demonstrated that Tseng and his colleagues authenticated encryption schemes are not secure in cases that the verifier substitutes his secret key, or when the verifier collaborates with another verifier and selects the measurable secret key for him. Their Cryptanalysis works only when the attack comes from system authority which contradicts the assumption made by Tseng and his colleagues [11] that system authority is trustworthy. However, in 2007, Chen and Jan [1] demonstrated that their attack cannot work. In the same year, Shao [9] presented an insider forgery attack to Tseng and his colleagues authenticated encryption scheme, and showed that their scheme cannot resist this attack. He also pointed out that this scheme is unable to achieve forward secrecy. Furthermore, he demonstrated another weakness of their schemes. Shao showed that these schemes do not have the nonrepudiation property. This means that in a case of dispute over the signed message the signer and receiver are unable to convince the third party that the message is valid. In 2005, Zhang and Feng [13] showed that Tseng and his colleagues schemes are insecure against existential forgery attack. At the same year, Tsai and his colleagues [10] showed that Tseng and his colleagues authenticated encryption scheme cannot withstand the known plaintext-ciphertext attack. This means that the assailant is able to expose all messages transmitted between the signer and his specified receiver. In 2006, Hwang and his colleagues [6] claimed that Tseng and his colleagues scheme is insecure against forgery attack. They also presented an improvement for the scheme to withstand the flaw. However, their proposed scheme was later shown to be insecure by Rasslan [8] in 2010. In 2008, Encinas and his colleagues [3] showed that Tseng and his colleagues authenticated encryption schemes and several other schemes based on this schemes suffer from a weakness affecting the authentication of signer's public key and the security of them. They also proposed some modifications in term of choosing the proper hash value for those schemes.

In this paper, man-in-the-middle attacks are proposed on both Tseng and his colleagues self-certified authenticated encryption schemes. It would be demonstrated that these schemes are unable to resist such attacks.

The rest of this paper is organized as follows. In section 2, the notion of signature scheme with message recovery is briefly reviewed. Section 3 is the review of the two variants of Tseng and his colleagues signature scheme. In section 4, these two schemes are shown to be insecure against man-in-the-middle attack. Eventually,

the conclusion is drawn in section 5.

2. Review of signature scheme with message recovery

In 1985, ElGamal [2] introduced a digital signature scheme based on discrete logarithm problem. In his scheme the message M should be sent as appendix with its signature.

In order to keep the message M confidential, and also to reduce communication overheads an ElGamal-like digital signature scheme was proposed by Neyberg and Ruppel [7]. In their scheme, the message M could be recovered from the digital signature directly. In 2003, Tseng and his colleagues [11] proposed the digital signature scheme with message recovery based on Neyberg and Ruppel's scheme. This scheme is performed in three phases.

2.1. System initialization phase

In the system initialization phase, there is a system authority (SA) that chooses and generates system parameters. The system authority first chooses two large prime numbers p and q of almost the same size such that $p = 2p' + 1$ and $q = 2q' + 1$. Then, he computes $N = p.q$. The system authority then chooses an integer g which is a base element of order $p'.q'$. The system authority keeps p, q, p', q' secret. He also publishes N and g, and a public one-way hash function h(.) which accepts the variant-length input string of bits and produces a fixed-length output string of bits as specified by NIST, which is $h(m) < \min(p', q')$. When a user U_i with the identity ID_i wants to join the system, he chooses a private key x_i randomly, and computes $p_i = g^{x_i} \, mod \, n$. Then, U_i sends p_i and ID_i to system authority. After receiving (p_i, ID_i), SA computes and publishes $U_i's$ public key $y_i = (p_i - ID_i)^{h(ID_i)^{-1}} mod \, n$. The user U_i can check the validity of his public key by verifying the equation $y_i^{h(ID_i)} + ID_i = g^{x_i} \, mod \, n.$

2.2. Signature generation phase

In this phase, the signer U_i wants to sign a message M which contains a predetermined redundancy. The signer U_i first chooses an integer k randomly. Then, U_i computes the signature (r, s) for the message M as follows.

$$r = M.g^{-k} \quad mod \, n$$

$$s = k - x_i.h(r)$$

Then, U_i sends (r, s) to the verifier.

2.3. Message recovery phase

After receiving (r, s), any user can use the public value y_i and ID_i to recover the message M as

$M = r.g^s.(y_i^{h(ID_i)} + ID_i)^{h(r)} \; mod \, n.$

The recovered message M must be verified by checking the validity of the embedded redundancy within it.

3. Tseng and his colleagues self-certified digital signature schemes with message recovery.

Tseng and his colleagues presented two variants for digital signature with message recovery. The first one is the authenticated encryption scheme that only allows the intended receiver to verify and recover the message. The other one is the authenticated encryption scheme with message linkages that is applicable for transmission of large messages.

3.1. Authenticated encryption scheme

Authenticated encryption scheme is the combination of two cryptographic protocols, encryption and digital signature. In this scheme only the specified receiver is able to recover and verify the message. Any other user is unable to do so. This scheme is also divided into three phases. The process of this scheme is given in Figure1.

3.1.1. System initialization phase

This phase is the same as system initialization phase in digital signature scheme with message recovery.

3.1.2. Signature generation phase

Suppose that a user U_i wants to sign and encrypt the message M containing enough redundancy to a specified receiver U_j. The signer U_i first chooses k at random. Then, he computes the signature (r, s) for the message M as follows

$$r = M.(y_j{}^{h(ID_j)} + ID_j)^{-k} \; mod \; n$$

$s = k - x_i.h(r)$.

Then, the signer U_i sends (r, s) to U_j.

3.1.3. Message recovery phase

Upon receiving (r, s), the specified receiver U_j first computes $g^k = g^s.(\,y_i{}^{h(ID_i)} + ID_i)^{h(r)} \; mod \; n$ $\mathrm{g^k = g^s.(y_i{}^{h(ID_i)} + ID_i)^{h(r)} mod n}$ $\mathrm{g^k = g^s.(y_i{}^{h(ID_j)} + ID_i)^{h(r)} mod n}$.

Then, he applies his private key x_j to compute $g^{kx_j} \; mod \; n$. Hence, U_j can recover M as $M = r.(g^s(\,y_i{}^{h(ID_i)} + ID_i)^{h(r)})^{x_j} \; mod \; n$. Then, the specified receiver U_j must check the validity of the recovered M for the embedded redundancy within it.

3.2. Authenticated encryption scheme with message linkages

This scheme is designed by Tseng and his colleagues for large messages which are divided into a sequence of message blocks. This scheme links up these message blocks to avoid message blocks being reordered, partially deleted, or replicated during transmissions. The process of the scheme is given in Figure2.

Phases	SA	U_i	U_j
System initialization phase		Chooses x_i randomly. Computes $p_i = g^{x_i} \bmod n.$ $SA \xleftarrow{(p_i, ID_i)} U_i$	
	Computes $y_i = (p_i - ID_i)^{h(ID_i)^{-1}} \bmod n.$ Publicize y_i. (does the same for any other user who joins the system)		
Signature generation phase		Chooses k randomly. Computes $r = M.(y_j{}^{h(ID_j)} + ID_j)^{-k} \bmod n$ $s = k - x_i.h(r)$ $U_i \xrightarrow{(r,s)} U_j$	
Message recovery phase			Computes $g^k = g^s (y_i{}^{h(ID_i)} + ID_i)^{h(r)} \bmod n$, and $M = r.(g^k)^{x_j} \bmod n.$ Checks the validity of the redundancy.

Figure 1: Tseng and his colleagues authenticated encryption scheme

3.2.1. System initialization phase

This phase is the same as the one presented in section 2.1.

3.2.2. Signature generation phase

Without the loss of generality, suppose that the signer U_i wants to sign and send the large message M to a specified receiver U_j.

This message is made up of the sequence $\{M_1,\ldots,M_n\}$ where $M_i \in GF(n)$, for $i = 1, \ldots, N$. In order to generate the signature for M, U_i performs the following procedure.

1. Let $r_0 = 0$, and choose k randomly.

2. Compute $t = (y_j{}^{h(ID_j)} + ID_j)^k \ mod \ n$.

3. Compute $r_i = M_i.h(r_{i-1} \oplus t) \ mod \ n$ for $i = 1, \ldots, N$, where $\oplus$denotes the exclusive operator.

4. Compute $s = k - x_i.r$, where $r = h(r_1 \parallel \cdots \parallel r_N)$, and "$\parallel$" denotes the concatenation operator.

Eventually, U_i sends $n + 2$ signature blocks $(r, s, r_1, \ldots, r_N)$ to U_j in a public way. Note that r_i is used as a linking parameter to generate ith and $(i + 1)$th message blocks.

3.2.3. Message recovery phase

Upon receiving the set $(r, s, r_1, \ldots, r_N)$, the receiver U_j performs the following verification procedure to recover the message blocks $\{M_1, \ldots, M_N\}$.

1. Compute $r' = h(r_1 \parallel r_2 \parallel \cdots \parallel r_N)$, and check that $r = r'$ holds or not.

2. Compute $g^k = g^s.(y_i{}^{h(ID_i)} + ID_i)^r \ mod \ n$, and the apply his own private key x_j to compute $g^{kx_j} \ mod \ n$ which is equal to t.

3. Recover the message blocks $\{M_1,\ldots,M_n\}$ as follows

$M_i = r_i.h(r_{i-1} \oplus t)^{-1} \ mod \ n$ for $i = 1,2, \ldots, N$, and $r_0 = 0$.

If the signer and receiver follow the procedure correctly, the message blocks $\{M_1, \ldots, M_N\}$ could be recovered precisely.

Phases	SA	U_i	U_j
System initialization phase		Chooses x_i randomly. Computes $p_i = g^{x_i} \bmod n.$ $SA \xleftarrow{(p_i, ID_i)} U_i$	
	Computes $y_i = (p_i - ID_i)^{h(ID_i)^{-1}} \bmod n.$ Publicize y_i.		
Signature generation phase		$r_0 = 0$, and chooses a random k, and computes $t = \left(y_j^{h(ID_j)} + ID_j\right)^k \bmod n$ $r_i = M_i . h(r_{i-1} \oplus t) \bmod n$ $r = h(r_1 \parallel \cdots \parallel r_N)$ $s = k - x_i . r$ $U_i \xrightarrow{(r, s, r_1, \ldots, r_N)} U_j$	
Message recovery phase			Computes $r' = h(r_1 \parallel r_2 \parallel \cdots \parallel r_N).$ Checks $r \stackrel{?}{=} r'$. Computes $g^k = g^s (y_i^{h(ID_i)} + ID_i)^r \bmod n$ $t = g^{k x_j} \bmod n$ $M_i = r_i . h(r_{i-1} \oplus t)^{-1} \bmod n$, and $r_0 = 0$.

Figure 2: Tseng and his colleagues authenticated encryption scheme with message linkage

4. Security analysis

Tseng and his colleagues provided a security analysis for their schemes in their paper. They discussed six possible attacks against their schemes, and claimed that none of those attacks could break their schemes. However, this does not guarantee that there exists no other attack that could jeopardize the security of these protocols. In the following subsections, man-in-the-middle attacks are represented to their schemes, and it will be shown that an invader is able to intercept the transmission and forge U_i's signature.

4.1. Man-in-the-middle attack on Tseng and his colleagues authenticated encryption scheme

A user U_i wants to sign a message M to the specified user U_j. The signature is (r, s). Suppose that A is a malicious attacker who intercepts the transmission without knowing the concealed message M. The procedure of attack is as follows. The process of the attack is given in Figure3.

1. After intercepting (r, s), A chooses l at random and computes

$$m = g^l \bmod n$$

$$s_A = s - l.h(r)$$

2. A chooses an identity ID_A, and computes $p_A = m.\left({y_i}^{h(ID_i)} + ID_i\right) mod\ n$, and sends (p_A, ID_A) to SA.

3. When SA receives (p_A, ID_A), he calculates the attacker's public key as

$$y_A = (p_A - ID_A)^{h(ID_A)^{-1}} \bmod n.$$

4. A sends (r, s_A) to U_j, and claims it as his legal signature for M.

The forged signature performs flawless in the message recovery phase since g^k can be calculated

$$g^k = g^{s_A}.({y_A}^{h(ID_A)} + ID_A)^{h(r)} \bmod n$$

, and M can be easily recovered by applying x_j

$$M = r.\left(g^{s_A}.\left({y_A}^{h(ID_A)} + ID_A\right)^{h(r)}\right)^{x_j} \bmod n$$

$$= r.(g^{s-l.h(r)}.(p_A)^{h(r)})^{x_j} \bmod n$$

$$= r(g^{s-l.h(r)}.(m.({y_i}^{h(ID_i)} + ID_i))^{h(r)})^{x_j} \bmod n$$

$$= r.(g^s.g^{-l.h(r)}.\left(g^{l.h(r)}.\left({y_i}^{h(ID_i)} + ID_i\right)\right)^{h(r)})^{x_j} \bmod n$$

$$= r.(g^s(y_i{}^{h(ID_i)} + ID_i))^{h(r)})^{x_j} mod\ n$$

4.2. Man-in-the-middle attack on Tseng and his colleagues authenticated encryption scheme with message linkages

Suppose U_i is the signer and he is attempting to sign the large message M which is divided to the sequence $\{M_1, \dots, M_N\}$ to the specified user U_j.

The signature is $(r, s, r_1, \dots, r_N)$. A is an attacker who intercepts the signature and forges a new signature without knowing the context of M. He forges a valid signature for M.

The process of the attack is shown in Figure4. The process of the attack is as follows.

1. After intercepting $(r, s, r_1, \dots, r_N)$, the attacker A chooses the number l at random and computes

$$m = g^l\ mod\ n$$

$$s_A = s - l.r$$

2. The attacker A chooses the identity ID_A, and computes

$$p_A = m.\left(y_i{}^{h(ID_i)} + ID_i\right)\ mod\ n$$

,and sends (p_A, ID_A) to SA.

3. After receiving (p_A, ID_A), the system authority (SA) computes attacker's public key as

$$y_A = (p_A - ID_A)^{h(ID_A)^{-1}} mod\ n$$

4. A sends $(r, s, r_1, \dots, r_N)$ to U_j as his legal signature for M .

SA	U_i	A	U_j
	Chooses $x_i$randomly.		
	Computes		
	$p_i = g^{x_i}\ mod\ n.$		
	$SA \xleftarrow{(p_i, ID_i)} U_i$		
Computes			
$y_i = (p_i - ID_i)^{h(ID_i)^{-1}} mod n.$			

Publicize y_i.

(does the same for any other user who joins the system)

Chooses k randomly.

Computes

$$r = M.(y_j^{h(ID)_j} + ID_j)^{-k} \bmod n$$

$$s = k - x_i.h(r)$$

$$U_i \xrightarrow{(r,s)}$$

A intercepts

Computes

$$m = g^l \bmod n$$

$$s_A = s - l.h(r)$$

$$p_A = m.(y_i^{h(ID_i)} + ID_i)^{h(r)}$$

$$SA \xleftarrow{(p_A, ID_A)} A$$

Computes

$$y_A = (p_A - ID_A)^{h(ID_A)^{-1}} \bmod n.$$

Publicizes y_A.

$$A \xrightarrow{(r,s_A)} U_j$$

Computes

$$g^k = g^{s_A}.(y_A^{h(ID_A)} + ID_A)^{h(r)} \bmod n$$

, and recovers

$$M = r.(g^k)^{x_j} \bmod n.$$

Checks the validity of the redundancy.

Figure 3: Man-in-the-middle attack on Tseng and his colleagues authenticated encryption scheme

SA	U_i	A	U_j
	Chooses $x_i$randomly.		
	Computes $p_i = g^{x_i} \bmod n.$		
	$\xleftarrow{(p_i, ID_i)}$		
Computes $y_i = (p_i - ID_i)^{h(ID_i)^{-1}}.$			
Publicize y_i.			
(does the same for any other user who joins the system)			
	$r_0 = 0$, and chooses k randomly.		
	Computes $t = (y_j^{h(ID_j)} + ID_j)^k \bmod n.$, and		
	$r_i = M_i.h(r_{i-1} \oplus t) \bmod n,$		
	$r = h(r_1 \parallel \cdots \parallel r_N),$		
	$s = k - x_i.r$		
		$\xrightarrow{(r, s, r_1, \ldots, r_N)}$	
			Computes $r' = h(r_1 \parallel r_2 \parallel \cdots \parallel r_N).$
			Checks $r \stackrel{?}{=} r'$.
			Computes $g^k = g^s(y_i^{h(ID_i)} + ID_i)^r \bmod n$ and $t = g^{kx_j} \bmod n$ $M_i = r_i.h(r_{i-1} \oplus t)^{-1} \bmod n$

Figure 4: Man-in-the-middle attack on Tseng and his colleagues authenticated encryption scheme with message linkages

The forged signature performs properly in the message recovery phase since g^k can be calculated as

$$g^{s_A}.({y_A}^{h(ID_A)} + ID_A)^r \ mod\ n = g^{s-lr}(p_A)^r \ mod\ n$$
$$= g^s.g^{-lr}.\left(m\left({y_i}^{h(ID_i)} + ID_i\right)^r\right) mod\ n$$
$$= g^s.g^{-lr}(g^{lr}\left(\left({y_i}^{h(ID_i)} + ID_i\right)^r\right)modn$$
$$= g^s\left({y_i}^{h(ID_i)} + ID_i\right)^r modn$$
$$= \ g^k \ mod\ n.$$

The reason of this attack affecting these two schemes is that in these two schemes the amount r in the signature contains the message in ciphertext, and the amount s contains the private key of signer. In both man- in-the-middle attacks, all that the attacker has to do is keeping r without change to protect the message M, and change the amount of s to forge a new signature with his own identity.

Note that in the first scheme $s = k - x_i.h(r)$, and the attacker is not aware of x_i. When he computes $s_A = s - l.h(r)$, he adds l to x_i since

$$s_A = s - l.h(r)$$
$$= k - x_i.h(r) - l.h(r)$$
$$= k - (x_i + l).h(r).$$

Therefore, to forge the message he only should choose a valid identity and p_A for s_A. Thus he chooses $g^{l+x_i} \ mod\ n$ as p_A (the same logic stands for the attack to the scheme with message linkages).

5. Conclusion

This paper reviews Tseng and his colleagues self-certified authenticated encryption schemes with message recovery. It provides man-in-the-middle attacks on both its variants, and shows that these schemes are vulnerable to this kind of attack. In both schemes a malicious attacker who is able to intercept the transmissions can forge a signature of a message without knowing the context of message. Thus, even though Tseng and his colleagues demonstrated that their schemes are secure against a number of possible attacks under the assumption that computing discrete logarithms modulo a large composite number and the one way hash function are difficult, they cannot resist man-in-the-middle attack.

References

[1] Y.-H. Chen and J.-K. Jan. “An authenticated encryption scheme for securely signing a signature with message linkages”, International Conference on Innovative Computing, Information and Control, pp. 77-80, 2007.

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

[3] L. H. Encinas and A.M Rey and J.M. Masque. “A Weakness in Authenticated Encryption Schemes Based on Tseng et al.’s schemes”, vol. 7, no. 2, pp. 185-187, 2008.

[4] M. Girault. “Self-certified public keys”, Advances in Cryptology—EUROCRYPT’91, Springer, Berlin, 1991, pp. 491-497.

[5] P. Horster and M. Michels and H. Petersen. “Authenticated encryption schemes with low communication costs”, Electronic Letters 30 (15), pp. 1212-1213, 1994.

[6] M. S. Hwang and J. Y. Hsiao and Y.-P. Chu. “Improvement of authenticated encryption schemes with message linkages for message flows”, IEICE Trans. Inf. & Syst., vol. E89-D, no.4, pp. 1575-1577, 2006.

[7] K. Neyberg and R. Ruppel. “Message recovery for signature schemes based on the discrete logarithm problem”, Advances in Cryptology—Erocryt’94, LNCS 950, Springer, Berlin, 1994, pp.175-190.

[8] M. Rasslan. “Cryptanalysis of Hwang-Lo-Hsiao-Chu Authenticated Encryption Schemes”, IEICE Trans. Inf. & Syst., vol. E93-D, no.5, pp. 1301-1302, 2010.

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

[10] C.-s. Tsai and S.-C. Lin and M.-S. Hwang. “Cryptanalysis of an authenticated encryption scheme using self-certified public keys”, Applied Mathematics and Computation 166, pp. 118-122, 2005.

[11] Y.-M. Tseng and J.-K. Jan and H.-Y. Chien. “Digital signature with message recovery using self-certified public keys and its variant.” Applied Mathematics and Computation 136, pp. 203-214, 2003.

[12] Q. Xie and Y. Xiu. “Cryptanalysis of Tseng et al.’s authenticated encryption schemes”, Applied Mathematics and Computation 158, pp. 1-5, 2004.

[13] Zh. Zhang and F. Feng, F. “Cryptanalysis of some signature schemes with message recovery”, Applied Mathematics and Computation 170, pp.103-114, 2005.