Computers and Electrical Engineering 37 (2011) 71–74

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Comments on the security of Chen's authenticated encryption scheme ☆

Mohamed Rasslan *, Amr Youssef

Concordia Institute for Information Systems Engineering, Concordia University, 1455 De Maisonneuve Blvd. West, Montreal, Quebec, Canada H3G 1M8

ARTICLE INFO

Article history:
Received 8 September 2009
Received in revised form 16 June 2010
Accepted 6 September 2010
Available online 20 October 2010

ABSTRACT

Chen (Computers and Electrical Engineering, vol. 30, 2004) illustrated that Tseng et al.'s authenticated encryption schemes, with message linkages for message flows, do not achieve their claimed integrity and authenticity properties. Furthermore, Chen presented some modified schemes to repair these flaws. In this paper, we show that the modified schemes proposed by Chen are not secure. In particular, we present an attack that allows a dishonest referee, in case of a dispute, to decrypt all the future and past authenticated ciphertext between the contended parties. We also present a simple fix to prevent this attack.

1. Introduction

Nyberg and Rueppel [1] proposed signature schemes with message recovery. Afterward, in [2] they also proposed a general procedure to modify all previously proposed signature schemes based on the discrete logarithm problem to allow for message recovery. Communication-wise, Nyberg and Rueppel's scheme was somewhat inefficient. Later on, Horster et al. [3] proposed an authenticated encryption scheme with a reduced communication cost. Since then, many "authenticated encryption" schemes have been proposed. In a strict sense, these schemes should be called signcryption schemes because their authors claim that they provide non-repudiation in addition to both authenticity and confidentiality, but we will follow the common terminology in the literature (e.g., [4–6]) and call them authenticated encryption schemes. Authenticated encryption schemes aim to simultaneously guarantee confidentiality, authenticity and non-repudiation properties. The confidentiality property ensures that the ciphertext does not reveal any secret information to an adaptive attacker given the infeasibility of breaking a mathematical assumption. The authenticity property ensures that an adaptive attacker cannot impersonate the legitimate sender/signer of a ciphertext/signature. The non-repudiation property ensures that a third party can resolve potential disputes between the sender and the recipient of a message in situations where the sender repudiates the generation of the signed ciphertext.

The "first-sign-then-encrypt" and "first-encrypt-then-sign" paradigms are early methods to implement authenticated encryption schemes [1,2,7,8]. These schemes achieve the non-repudiation property, but they are costly in terms of communication and computation requirements. On the other hand, schemes that simultaneously combine the authenticity and confidentiality operations (e.g., [3,6,9]) are usually more efficient in terms of their communication and computation requirements. For more details regarding efficient authenticated encryption schemes and their pros and cons, we refer the reader to [10–16]. In these schemes, the sender (signer) generates a signature on a message and then sends the signature to a designated recipient (verifier). The designated verifier is the only one who can recover and verify the message. Typically, authenticated encryption schemes allow the signer to split the message into several blocks. Hence, the signer needs to perform the encryption and sign for each message block individually. Schemes with the message splitting feature require opti-

☆ Reviews processed and proposed for publication by Deputy Editor Dr. F. Sahin.

* Corresponding author. Tel.: +1 514 848 2424; fax: +1 514 848 3171.
E-mail address: m_rassla@encs.concordia.ca (M. Rasslan).

0045-7906/$ - see front matter © 2010 Published by Elsevier Ltd.
doi:10.1016/j.compeleceng.2010.09.001

mized computing and efficient bandwidth usage. Both [5,6] are examples of authenticated encryption schemes with message linkage properties. Communication-wise and computation-wise, Tseng et al.'s schemes [6] are more efficient than all the previously presented schemes. They proposed two authenticated encryption schemes with message linkages. The first scheme is a basic one and requires the recipient (verifier) to wait until she receives all of the signature blocks before she can recover the message blocks. The second scheme is a generalized one and allows the recipient (verifier) to recover the message blocks upon receiving their corresponding signature blocks. Tseng et al.'s generalized scheme is perfect for some application requirements and it is designed for packet switched networks.

Unfortunately, Chen [17] showed that this authenticated encryption scheme does not achieve its claimed integrity and authenticity properties. To overcome this security breach, Chen proposed a modification to these schemes [17]. In this paper, we show that the modified schemes proposed by Chen are not secure. In particular, we present an attack that allows the referee, in case of a dispute, to decrypt all the authenticated traffic between the sender(signer) and the designated recipient of the authenticated ciphertext.

The remainder of this paper is organized as follows. In the next section, we briefly review the details of Chen's scheme that are relevant to our attack scenario. Our proposed attack is described in Section 3. In Section 4, we present a modification to Chen's scheme to prevent our attack. Finally, we conclude in Section 5.

2. Chen's improved authenticated encryption schemes

In this section, we briefly review the relevant details of the authenticated encryption schemes proposed by Chen. We introduce the basic scheme only. However, our attack is also applicable to the generalized scheme. For further details about these schemes, the reader is referred to [17].

Similar to Tseng et al. [6], the improved scheme proposed by Chen consists of three phases: the system initialization phase, the signature generation phase, and the message recovery phase.

System initialization phase: The system authority (SA) selects a large prime p such that $p-1$ has a large prime factor q. SA also picks an integer, g, with order q in $GF(p)$. Let f denote a secure one-way hash function. The SA publishes p, q, g, and f. Each user, U_i, chooses a secret key $x_i \in Z_q$ and computes the corresponding public key $y_i = g^{x_i} \bmod p$.

Signature generation phase: The signer U_a wants to securely send the designated recipient U_b a large authentic message. The signer splits the message M into the sequence $\{M_1, M_2, \ldots, M_n\}$, where $M_i \in GF(p)$. Then, the signer U_a performs the following operations to generate the signature blocks for the message M:

(1) Pick a random number $k \in Z_q^*$ and set $r_0 = 0$, then compute

$$y_b^k \bmod p \tag{1}$$

(2) Compute

$$r_i = M_i \cdot f(r_{i-1} \oplus y_b^k) \bmod p \tag{2}$$

for $i = 1, \ldots, n$, where $\oplus$ denotes the exclusive-or operator.

(3) Compute

$$s = k \cdot R - r \cdot x_a \bmod q \tag{3}$$

where $R = g^k \bmod p$, $r = f(r_1 \| r_2 \| \cdots \| r_n)$, and $\|$ denotes the concatenation operator.

The signature for the message M is $(R, r, s, r_1, \ldots, r_n)$.

Finally, U_a sends these $(n+3)$ authenticated ciphertext blocks to U_b over the insecure channel.

The message recovery phase: After the designated recipient U_b receives the signature blocks $(R, r, s, r_1, \ldots, r_n)$, she performs the following operations on them to recover the message blocks $\{M_1, M_2, \ldots, M_n\}$.

(1) Compute $r' = f(r_1 \| r_2 \| \cdots \| r_n)$, and check whether $r' = r$ or not.

(2) Verify

$$R^R \overset{?}{=} g^s \cdot y_a^r \bmod p. \tag{4}$$

(3) Compute

$$y_b^k = R^{x_b} \bmod p. \tag{5}$$

(4) Recover the message blocks $\{M_1, M_2, \ldots, M_n\}$ as follows

$$M_i = r_i \cdot f(r_{i-1} \oplus y_b^k)^{-1} \bmod p \tag{6}$$

for $i = 1, \ldots, n$ and $r_0 = 0$.

3. The proposed attack

In this section we introduce our attack on Chen's schemes. Our attack shows that, in case of a dispute, the involved third party (referee) can decrypt all the future and past traffic between the contended parties. Consider the case where a verifier U_b wants to convince a third party (referee) that she is the designated recipient of the signature blocks that originate from the signer (encrypter) U_a.

In other words, U_b wants to achieve the non-repudiation property. So, she reveals y_b^k to the referee. Then U_b proves (e.g., using zero knowledge protocol [18]) to the referee that she knows the discrete logarithm of R to $y_b^k \bmod p$. Given the signature blocks $(R, r, s, r_1, \ldots, r_n)$, the referee carries out the following steps:

(1) Calculate $r' = f(r_1 \| r_2 \| \cdots \| r_n)$, and check whether $r' = r$ or not.
(2) Verify that

$$R^R \overset{?}{=} g^s \cdot y_a^r \bmod p \tag{7}$$

The knowledge of $y_b^k \bmod p$ and the signature blocks $(R, r, s, r_1, \ldots, r_n)$ allow the referee to calculate $y_{ab} \bmod p$ as follows: First, she raises y_b to s and re-orders the exponents and bases as in the following equation:

$$\begin{aligned} y_b^s &= y_b^{k \cdot R - r \cdot x_a} \bmod p \\ &= y_b^{k \cdot R} \cdot y_{ab}^{-r} \bmod p \end{aligned} \tag{8}$$

Then, she drives y_{ab}^r as follows:

$$y_{ab}^r = y_b^{k \cdot R} \cdot y_b^{-s} \bmod p \tag{9}$$

Finally, she calculates y_{ab} as follows:

$$y_{ab} = \left(y_b^{k \cdot R} \cdot y_b^{-s}\right)^{r^{-1}} \bmod p \tag{10}$$

Later, the referee can intercept the traffic between U_a and U_b. Hence, she can decrypt the signature blocks as follows:

(1) Assume that the new signature blocks are $(R', r', s', r_1', \ldots, r_n')$, where $R' = g^{k'} \bmod p$. The attacker (i.e., the dishonest former referee) calculates $R' = y_b^{k'} \bmod p$ to perform the decryption. So, she raises y_b to s' and re-orders the exponents and bases as in the following equation:

$$y_b^{s'} = y_b^{k' \cdot R' - r' \cdot x_a} \bmod p \tag{11}$$

Then,

$$\begin{aligned} y_b^{k' \cdot R'} &= y_b^{s'} \cdot y_b^{r' \cdot x_a} \bmod p \\ &= y_b^{s'} \cdot y_{ab}^{r'} \bmod p \end{aligned} \tag{12}$$

Finally, she calculates $y_b^{k'} \bmod p$ as follows:

$$y_b^{k'} = \left(y_b^{s'} \cdot y_{ab}^{r'}\right)^{R'^{-1}} \bmod p \tag{13}$$

where R'^{-1} is the multiplicative inverse of $R' \bmod q$.
(2) The attacker recovers the message blocks $\{M_1', M_2', \cdots, M_n'\}$ as

$$M_i' = r_i' \cdot f\left(r_{i-1}' \oplus y_b^{k'}\right)^{-1} \bmod p \tag{14}$$

for $i = 1, \ldots, n$ and $r_0' = 0$.

As demonstrated above, targeting the non-repudiation allows the referee to decipher the ciphertext between U_a and U_b. The same attack also applies to the generalized form of Chen's scheme.

4. Preventing the attack

As illustrated in the previous section, when a dispute takes place between the signer U_a and the verifier U_b, U_b reveals y_b^k and the message M to the referee in order to allow the referee to verify that

$$M_i = r_i \cdot f\left(r_{i-1} \oplus y_b^k\right)^{-1} \bmod p$$

for $i = 1, \ldots, n$ and $r_0 = 0$.

The knowledge of y_b^k leads up to the loss of both the forward and backward secrecy properties. This is due the fact that the referee can calculate the shared secret key, y_{ab}, between U_a and U_b. Hence, the referee can decrypt all the future and past traffic between the contended parties. Ensuring that there is no possible dispute between U_a and U_b would prevent our attack. However, this assumption is not realistic in many practical situations. One way to prevent this attack is to modify the way r_i is computed as follows (instead of Eq. (2)):

$$r_i = M_i \cdot f\left(r_{i-1} \oplus f\left(y_b^k\right)\right) \mod p \tag{15}$$

for $i = 1, \ldots, n$.

Consequently, in the message recovery phase we also modify the way M_i is computed as follows (instead of Eq. (6)):

$$M_i = r_i \cdot f\left(r_{i-1} \oplus f\left(y_b^k\right)\right)^{-1} \mod p \tag{16}$$

for $i = 1, \ldots, n$ and $r_0 = 0$.

In case of a dispute, U_b reveals $f(y_b^k)$ instead of y_b^k to the referee. Given $f(y_b^k)$, the referee can verify that

$$r_i = M_i \cdot f\left(r_{i-1} \oplus f\left(y_b^k\right)\right) \mod p$$

for $i = 1, \ldots, n$.

At the same time, the referee cannot drive y_{ab} from Eq. (10). Furthermore, given the one-wayness property of f, it is infeasible to drive y_b^k from $f(y_b^k)$.

5. Conclusion

The "*improved*" authenticated encryption scheme proposed by Chen is not secure. A dishonest arbitrator can decrypt all future and past traffic between contended parties which contradicts the forward and backward confidentiality requirements.

References

[1] Nyberg K, Rueppel RA. A new signature scheme based on the DSA giving message recovery. In: First ACM conference on computer and communications security, Fairfax, Virginia; 1993. p. 58–61.

[2] Nyberg K, Rueppel RA. Message recovery for signature schemes based on the discrete logarithm. Des Codes Cryptogr 1996;7(1–2):61–81.

[3] Horster P, Michels M, Petersen H. Authenticated encryption schemes with low communication costs. Electron Lett 1994;30(15):212–1213.

[4] Zhang Z, Araki S, Xiao G. Improvement of authenticated encryption schemes with message linkages for message flows. Appl Math Comput 2005;162(3):1475–83.

[5] Lee W-B, Chang C-C. Authenticated encryption schemes with linkage between message blocks. Inf Process Lett 1977;63(5):47–250.

[6] Tseng Y-M, Jan J-K, Chien H-Y, flows Authenticated encryption schemes with message linkages for message. Comput Elect Eng 2003;29(1):101–9.

[7] Kohnfelder LM. On the signature reblocking problem in public key cryptosystems. Commun ACM 1995;31(19):1656–7.

[8] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21(2):120–6.

[9] Lee W-B, Chang C-C. Authenticated encryption schemes without using a one way function. Electron Lett 1995;31(19):1656–7.

[10] Lee M, Kim D, Park K. An authenticated encryption scheme with public verifiability. Japan–Korea Joint Workshop Algorithms Comput (WAAC2000), 2000. p. 49–56.

[11] Hwang M-S, Chang C-C, Hwang K-F. An ElGamal-like cryptosystem for enciphering large messages. IEEE Trans Knowl Data Eng 2002;14(2):445–6.

[12] Hwang M-S, Liu C-Y. Authenticated encryption schemes: current status and key issues. Int J Network Security 2005;1(2):61–73.

[13] Nyberg K, Rueppel RA. Message recovery for signature schemes based on the discrete logarithm. Adv Cryptology Eurocrypt'94 1994:175–90.

[14] Wu T-S, Wu T-C, He W-H. Authenticated encryption schemes with double message linkage. In: Proceedings of the 9th national conference on information security, ROC; 1999. p. 303–8.

[15] Chen K. Authenticated encryption schemes based on quadratic residue. Electron Lett 1998;34(22):2115–6.

[16] Hsu C-L, Wu T-C. Authenticated encryption schemes with (t, n) shared verification. IEE Process Comput Digit Technol 1998;145(2):117–20.

[17] Chen B-H. Improvement of authenticated encryption schemes with message linkages for message flows. Comput Elect Eng 2004;30:465–9.

[18] Boyer J, Chaum D, Damgard I, Pederson T. Convertable undeniable signatures. Crypto'90 1991:189–205.