Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 19 (2013) 565 – 569

Procedia Computer Science

The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013)

On the Security of Hwang-Lo-Hsiao-Chu Authenticated Encryption Schemes

Mohamed Rasslan*

Abstract

In 2006, Hwang *et al.* presented a forgery attack against Tseng *et al.*'s efficient authenticated encryption schemes with message linkages for message flows. Moreover, they proposed some modified schemes to repair these flaws. In this paper, we show that the improved authenticated encryption schemes proposed by Hwang *et al.* are insecure by presenting another attack that allows a dishonest referee, dealing with a dispute, to decrypt all the future and past authenticated ciphertext between the contending parties. This attack proves that Hwang *et al.*'s schemes contradict the forward and backward confidentiality requirements of authenticated encryption schemes.

Selection and peer-review under responsibility of Elhadi M. Shakshuki

Keywords: Authenticated encryption, confidentiality, non-repudiation, cryptanalysis.

1. Introduction

Typical authenticated encryption schemes guarantee confidentiality, authenticity (unforgeability) and non-repudiation properties [1, 2]. Several authenticated encryption schemes have been proposed in the literature to achieve theses three essential requirements. Nyberg and Rueppel [1, 3] proposed the first authenticated encryption scheme with message recovery. To improve upon the communication and computation complexities of the original Nyberg and Rueppel scheme, several variants of authenticated encryption schemes have been proposed. For example, the schemes in [3, 4, 5] achieve these requirements, but they are costly in terms of their communications and computations overhead. On the other hand, schemes that simultaneously combine the authenticity and the confidentiality operations are more efficient [6]. For more details regarding efficient authenticated encryption schemes and their advantages and disadvantages, we refer the reader to [7, 8, 9, 10, 11, 12, 13].

Tseng *et al.* [6] proposed an efficient authenticated encryption scheme and its generalization, both with message linkages. The first scheme is a basic one that requires the recipient (verifier) to wait until she receives all of the signature blocks before she can recover any of the received message blocks. The second scheme is a generalized one that allows the recipient to recover the message blocks upon receiving their

*Corresponding author
Email address: m_rassla@encs.concordia.ca (Mohamed Rasslan)

Selection and peer-review under responsibility of Elhadi M. Shakshuki
doi:10.1016/j.procs.2013.06.075

corresponding signature blocks. This makes it an attractive choice in many applications such as packet switched networks. Unfortunately, Hwang *et al.* [14] showed that these authenticated encryption schemes do not fulfill claims to their integrity and authenticity properties. To overcome these security problems, Hwang *et al.* proposed a modification of these schemes [14].

In this paper, we show that the modified schemes proposed by Hwang *et al.* do not overcome the shortcomings of the original Tseng *et al.* scheme. In particular, we present an attack that allows the referee, dealing with a dispute, to decrypt all the authenticated traffic between the 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 Hwang *et al.*'s schemes that are relevant to our attack. Our proposed attack is presented in section 3. Finally we offer concluding comments in section 4.

2. Hwang *et al.* improved authenticated encryption schemes

In this section, we briefly review the relevant details of the authenticated encryption schemes proposed by Hwang *et al.* For further details about these schemes, the reader is referred to [14].

Similar to Tseng *et al.* [6], the improved schemes proposed by Hwang *et al.* consist of three phases: the system initialization phase, the signing phase, and the message recovery phase. Here, we focus only on the basic scheme but our attack equally applies to the generalized scheme.

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 $f(\cdot)$ be a secure one-way hash function. The SA publishes p, q, g, and $f(\cdot)$. Each user, U_i, chooses a secret key $x_i \in Z_q^*$ and computes the corresponding public key $y_i = g^{x_i} \bmod p$.

To overcome the weaknesses in Tseng *et al.*'s scheme, Hwang *et al.* require the signer U_a to send $t = g^k \bmod p$ in addition to s, and $r_1, r_2, \ldots, r_n$ to the verifier U_b. Hwang *et al.*'s scheme then proceeds as follows:

The Signing Phase: When the signer U_a wants to send the authenticated encrypted message M to a designated recipient U_b, she divides the message M into the sequence $\{M_1, M_2, \cdots, M_n\}$, 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 $y_b^k \bmod p$ and $t = g^k \bmod p$.

(2) Compute

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

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

(3) Compute

$$s = k - r \cdot x_a \bmod q \tag{2}$$

where $r = f(r_1 \| r_2 \| \cdots \| r_n)$, and $\|$ denotes the concatenation operator.

Finally, U_a sends $(n+2)$ signature blocks $(t, s, r_1, r_2, \ldots, r_n)$ to U_b over the insecure channel.