LETTER

Cryptanalysis of Hwang-Lo-Hsiao-Chu Authenticated Encryption Schemes

Mohamed RASSLAN[†a)], *Member and* **Amr YOUSSEF**[††], *Nonmember*

SUMMARY Tseng et al. proposed two efficient authenticated encryption schemes with message linkages for message flows. Hwang et al. (IEICE Trans. Inf. and Syst., Vol. E89-D, No. 4, April 2006) presented a forgery attack against these two schemes and proposed an improvement that they claim resists such attacks. In this paper, we show that the improved authenticated encryption schemes proposed by Hwang et al. are not secure by presenting another message forgery attack against these improved schemes.

key words: *authenticated encryption, authenticity, non-repudiation*

1. Introduction

Authenticated encryption schemes are encryption systems which aim to simultaneously achieve both privacy and authenticity of communications. Several authenticated encryption schemes have been proposed in the literature. Nyberg and Rueppel [1], [2] proposed the first authenticated encryption scheme with message recovery based on the discrete logarithm problem. To improve upon the communication and computation complexities of the original Nyberg and Rueppel scheme, several variants of authenticated encryption schemes have been proposed (e.g., [3]–[11]).

Tseng et al. [12] proposed two efficient authenticated encryption schemes 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 signature blocks. This makes it an attractive choice in many applications such as packet switched networks. Unfortunately, Hwang et al. [13] showed that these authenticated encryption schemes do not fulfill their claimed integrity and authenticity properties. To overcome these security problems, Hwang et al. proposed a modification to these schemes [13].

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 a message forgery attack that allows the adversary to alter the message flow and pass the integrity check by the verifier.

Manuscript received August 28, 2009.

[†]The author is with the Electrical and Computer Engineering Department, Concordia University, Montreal, Quebec, Canada.

[††]The author is with Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada.

a) E-mail: m_rassla@encs.concordia.ca

DOI: 10.1587/transinf.E93.D.1301

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 described in Sect. 3. Finally we conclude in Sect. 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 [13].

Similar to Tseng et al. [12], 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 only focus on the basic scheme but our attack also 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 $r_i = M_i \cdot f(r_{i-1} \bigoplus y_b^k) \bmod p$ for $i = 1, \ldots, n$, where $\bigoplus$ denotes the exclusive-or operator.

(3) Compute $s = k - r \cdot x_a \bmod q$, 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.

The Message Recovery Phase: After the designated recipient U_b receives all the signature blocks

Copyright © 2010 The Institute of Electronics, Information and Communication Engineers

$(t, s, r_1, r_2, \ldots, r_n)$, she performs the following operations on them to recover the message blocks $\{M_1, M_2, \cdots, M_n\}$.
(1) Compute $r' = f(r_1 \| r_2 \| \cdots \| r_n)$. Then, check whether $t^{x_b} \stackrel{?}{=} y_b^s y_{ab}^{r'} \bmod p$ holds, where $y_{ab} = y_a^{x_b} \bmod p$. If $t^{x_b} = y_b^s y_{ab}^{r'} \bmod p$ holds, then U_b moves to the second step.
(2) Recover the message blocks $\{M_1, M_2, \cdots, M_n\}$ as $M_i = r_i \cdot f(r_{i-1} \bigoplus t^{x_b})^{-1} \bmod p$, for $i = 1, \ldots, n$ and $r_0 = 0$.

3. The Proposed Attack

The following attack illustrates how an adversary can forge valid signature blocks that pass the recipient's verification.

The Signing Phase: Assume that the adversary intercepts some signature blocks $(t, s, r_1, r_2, \ldots, r_n)$ that were previously sent from U_a to U_b. The adversary can then alter the message flow as follows:
(1) Generate random r_i', $1 \le i \le n$.
(2) Calculate $r' = f(r_1' \| r_2' \| \cdots \| r_n')$.
(3) Calculate $t' = t \cdot y_a^{-(r-r')} \bmod p$.
(4) Send $(t', s, r_1', r_2', \ldots, r_n')$ to U_b.

The Message Recovery Phase: The designated recipient U_b calculates $r'' = f(r_1' \| r_2' \| \cdots \| r_n') = r'$. Then, U_b verifies that

$$t'^{x_b} \stackrel{?}{=} y_b^s y_{ab}^{r''} \bmod p \tag{1}$$

where $y_{ab} = y_a^{x_b} \bmod p$.

Our forgery attack ensures that U_b finds that the left hand side $t'^{x_b} \bmod p$ is equal to the right hand side $y_b^s y_{ab}^{r''} \bmod p$. Therefore, U_b recovers the forged message blocks $\{M_1', M_2', \cdots, M_n'\}$ as:

$$M_i' = r_i' \cdot f(r_{i-1}' \bigoplus t'^{x_b})^{-1} \bmod p, \tag{2}$$

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

The correctness of the proposed attack follows by noting that

$$\begin{aligned} t'^{x_b} &= (t \cdot y_a^{-(r-r')})^{x_b} \bmod p \\ &= t^{x_b} \cdot y_a^{-x_b \cdot (r-r')} \bmod p \\ &= g^{k \cdot x_b - x_a \cdot x_b \cdot (r-r')} \bmod p \end{aligned} \tag{3}$$

$$\begin{aligned} y_b^s y_{ab}^{r'} &= y_b^{k - r \cdot x_a} g^{x_a \cdot x_b \cdot r'} \bmod p \\ &= g^{x_b \cdot (k - r \cdot x_a)} g^{x_a \cdot x_b \cdot r'} \bmod p \\ &= g^{x_b \cdot k - x_a \cdot x_b \cdot r} g^{x_a \cdot x_b \cdot r'} \bmod p \\ &= g^{k \cdot x_b - x_a \cdot x_b \cdot (r-r')} \bmod p \end{aligned} \tag{4}$$

4. Conclusion

The improved authenticated encryption scheme proposed by Hwang et al. is not secure. Although in some situations the verifier might be able to decide whether the recovered message is meaningful or not, she still has to perform the decryption operations to make this decision. Because of the computational complexity associated with these decryption operations, an attacker can easily drive the network into a denial of service mode by over-flooding the communication links with forged message flows.

References

[1] K. Nyberg and R.A. Rueppel, "A new signature scheme based on the DSA giving message recovery," 1st ACM Conference on Computer and Communications Security, pp.58–61, Fairfax, Virginia, Nov. 1993.
[2] K. Nyberg and R.A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," Advances in Cryptology, Eurocrypt'94, pp.175–190, 1994.
[3] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," Electron. Lett., vol.30, no.15, pp.1212–1213, 1994.
[4] M.-S. Hwang, C.-C. Chang, and K.-F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," IEEE Trans. Knowl. Data Eng., vol.14, no.2, pp.445–446, 2002.
[5] M.-S. Hwang and C.-Y. Liu, "Authenticated encryption schemes: Current status and key issues," Int. J. Network Security, vol.1, no.2, pp.61–73, 2005.
[6] W.-B. Lee and C.-C. Chang, "Authenticated encryption schemes with linkage between message blocks," Inf. Process. Lett., vol.63, no.5, pp.247–250, 1977.
[7] K. Nyberg and R.A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," Des., Codes Cryptogr., vol.7, no.1-2, pp.61–81, 1996.
[8] T.-S. Wu, T.-C. Wu, and W.-H. He, "Authenticated encryption schemes with double message linkage," Proc. 9th National Conference on Information Security, pp.303–308, R.O.C., 1999.
[9] K. Chen, "Authenticated encryption schemes based on quadratic residue," Electron. Lett., vol.34, no.22, pp.2115–2116, 1998.
[10] W.-B. Lee and C.-C. Chang, "Authenticated encryption schemes without using a one way function," Electron. Lett., vol.31, no.19, pp.1656–1657, 1995.
[11] C.-L. Hsu and T.-C. Wu, "Authenticated encryption schemes with (t, n) shared verification," IEE Proc., Comput. Digit. Tech., vol.145, no.2, pp.117–120, 1998.
[12] Y.-M. Tseng, J.-K. Jan, and H.-Y. Chien, "Authenticated encryption schemes with message linkages for message flows," Computers and Electrical Engineering, vol.29, no.1, pp.101–109, 2003.
[13] M.-S. Hwang, 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, April 2006.