An Improvement on Secure E-mail Protocols Providing Perfect Foward Secrecy

Iuon-Chang Lin[1] Yang-Bin Lin[2] Chung-Ming Wang[2]

Department of Management Information Systems[1]
National Chung Hsing University, Taichung, Taiwan

Department of Computer Science[2]
National Chung Hsing University, Taichung, Taiwan

Abstract

In 2005, Sun, Hsieh, and Hwang proposed two secure e-mail protocols with perfect forward secrecy. In the first protocol, the authors apply smart card and Diffie-Hellman key agreement scheme to achieve the perfect forward secrecy. However, due to it requires a smart card to store some parameters, it is not practical in the real world. Thus, the authors proposed another protocol without a smart card. However, the second protocol has a security flaw in providing perfect forward secrecy. In this paper, we shall not only point out the secure flaw in the second protocol but also propose an improvement scheme to overcome the security flaw.

Keywords: E-mail, perfect forward secrecy, smart card, Diffie-Hellman key agreement

1 Introduction

Nowadays E-mail has been widely used in communications. However, to transmit messages in an open network is insecure. Attackers can easy intercept the transmitted messages from network. In order to prevent the confidentiality of transmitted messages from unauthorized access, people or systems usually encrypt the transmitted messages to obtain confidentiality. The existing E-mail systems [1, 6] apply public-key cryptosystem to encrypt a secure key and apply symmetric cryptosystem with the secret key to encrypt the transmitted messages. For example, a sender Bob wants to communicates with a receiver Alice by using the E-mail system. First, the E-mail system encrypts the transmitted message M using a short-term secret key k. The produced ciphertext is $E_k[M]$, where $E_k[]$ stands for a symmetric encryption function using a secret key k. Next, the system encrypts the secret key k using Alice's public-key pk, and generates the ciphertext $Enc_{pk}[k]$, where $Enc_{pk}[]$ stands for public-key encryption function using a public key pk. Then the system transmits $Enc_{pk}[k]$ and $E_k[M]$ to Alice over a network. Upon receiving $Enc_{pk}[k]$ and $E_k[M]$, Alice decrypts $Enc_{pk}[k]$ using her private key sk to obtain the short-term secret key k. Then, Alice decrypts $E_k[M]$ using the secret key k. However, the system can not provide the perfect forward secrecy. Perfect forward secrecy is defined as a protocol and is said to have a perfect forward secrecy if compromised of the long-term keys it does not compromise the past session keys [5]. Therefore, if a scheme satisfies the property of the perfect forward secrecy, it is more secure [4, 9, 10].

In 2005, Sun, Hsieh, and Hwang [8] proposed two secure e-mail protocols with the perfect forward secrecy. The first protocol applied Diffie-Hellman key agreement scheme [2] and a smart card to achieve perfect forward secrecy. The second protocol applied ElGamal crytposystem [3] and Shnorr's [7] signature scheme to design the protocol. The authors claimed that the two protocols provided perfect forward secrecy. However, we find that the second protocol has a security flaw. In this paper, we shall point out the security flaw in Sun, Hsieh, and Hwang's scheme. In addition, we also propose an improved protocol to eliminate the security flaw.

The rest of this paper is organized as follows. In the next section, we will review Sun, Hsieh, and Hwang's scheme and point out the security flaw in their protocol. An improved scheme is proposed in Section 3. Finally, we will make a brief conclusion in Section 4.

2 Review of Sun, Hsieh, and Hwang's Scheme

In this section, we will describe two protocols proposed by Sun, Hsieh, and Hwang [8] in 2005. Before describing the two protocols, we first define some symbols which will be used later.

- $Sig_k(M)$: A signature of message M using a private key k.
- $E_k[M]$: An encryption of the message M using a symmetric cryptosystem with a secret key k.
- A, B: The receiver and the sender, respectively.
- p: A large prime number.
- $h()$: A one-way hash function.
- $Cert$: A certificate of the ciphertext.
- $Enc_{pk}(M)$: An encryption of the message M using a public-key cryptosystem with a public key pk.
- k_a, k_b, and k_{ms}: The secret keys of A, B, and mail server, respectively.

2.1 Secure Protocol for E-mail System Using Smart Card

In this section, we will describe the secure E-mail protocol using smart card. The details of the protocol are as follows.

Step 1 (B is off-line): A selects a random number x, and sends $g^x \bmod p$ and $Sig_{k_a}(g^x \bmod p)$ to mail server.

Step 2 (A is off-line): B also selects a random number y, and sends $Sig_{k_b}(g^y \bmod p)$, $g^y \bmod p$, and ID_A to mail server.

Step 3 (A is off-line): Mail server sends $g^x \bmod p$ and $Sig_{k_a}(g^x \bmod p)$ to B. Then, B can compute the encryption key $k = (g^x)^y \bmod p$.

Step 4 (A is off-line): B encrypts message M using a key k obtained by step three, and then sends $E_k[M]$ and $h(k||g^x \bmod p)$ to mail server.

Step 5 (B is off-line): A requests mail server for new mail, and mail server will ask A to enter his ID and *password*. If A's ID and *password* are all correct, A can receive the new mail. Mail sever sends $h(k||g^x \bmod p)$, $g^y \bmod p$, $Sig_{k_b}(g^y \bmod p)$, and $E_k[M]$ to A.

Step 6 (B is off-line): In order to decrypt the message M, A must have a decryption key. A computes the decryption key $k = (g^y)^x \bmod p$. Finally, A uses the decryption key k to decrypt $E_k[M]$.

In this protocol, the authors applied the principle of Diffie-Hellman key exchange and agree with the the decryption key and encryption key. Since $k = g^{xy} \bmod p$, we can find that the decryption key and the encryption key are identical. The protocol can achieve the perfect forward secrecy, but A has to use a device, such as a smart card, to memorize a random number x to compute the decryption key k.

2.2 Secure Protocol for E-mail System without Using Smart Card

In this section, we will describe the second protocol without using a smart card. For the sake of making sure that a ciphertext is certainly someone's signature without letting on the signature, the concept of Certificate of Encrypted Message Being a Signature(CEMBS) is used as a second protocol. In addition, ElGamal cryptographic system [3] and Shnorr's signature scheme [7] are employed to achieve the perfect forward secrecy. The details for a second protocol are as follows.

Step 1 (A is off-line): B produces a signature $Sig_{k_b}(ID_A) = (r, s)$ by using Shnorr's signature scheme [7], where $r = g^x \bmod p$ and $s = b + h(ID_A, r) \bmod p - 1$. Next, B encrypts r by using ElGamal cryptosystem [3]. The generated ciphertext is $Enc_{PK_A}(r) = (W, V)$, where $W = g^w \bmod p$ and $V = r(PK_A)^w \bmod p$ in which w is a random number and PK_A denotes $A's$ public key. Then, B sends $Enc_{PK_A}(r)$, ID_A, and $Cert$ to mail server. $Cert$ is used to certify that ciphertext is indeed someone's signature without revealing the signature.

Step 2 (A is off-line): The mail server sends $g^y \bmod p$ and $Sig_{k_{ms}}(g^y \bmod p)$ to B.

Step 3 (A is off-line): After receiving $g^y \bmod p$ and $Sig_{k_{ms}}(g^y \bmod p)$, B can check whether $g^y \bmod p$ was tampered with during transmission by using mail server's public key to verify $Sig_{k_{ms}}(g^y \bmod p)$. If it holds, B computes the encryption key $k = (g^y)^x \bmod p$, and encrypts the message with the encryption key k. Next, B sends $E_k[M]$ and $h(k||g^y \bmod p)$ to the mail server.

Step 4 (B is off-line): A asks mail server for new mails, and mail server asks A to input his Id and password. If the Id and password are correct, the

mail server delivers $Enc_{PK_A}(r)$, $Cert$, $E_k[M]$, $h(k||g^y \bmod p)$, and $Enc_{Pk_{psd}}(y)$ to A.

Step 5 (B is off-line): After receiving $Enc_{PK_A}(r)$, $Cert$, $E_k[M]$, $h(k||g^y \bmod p)$, and $Enc_{Pk_{psd}}(y)$, A decrypts the $Enc_{Pk_{pwd}}(y)$ by utilizing his password, and obtains a random number y. Next, A utilizes his secret key to decrypt $Enc_{PK_A}(r)$, and obtains $r = g^x \bmod p$.

Step 6 (B is off-line): A computes the decryption key $k = r^y = (g^x)^y \bmod p$. Further, A can verify whether decryption key k is valid or not by $h(k||g^y \bmod p)$. If it is valid, a message can be decrypted with the decryption key k.

2.3 Remarks on Sun, Hsieh, and Hwang's Scheme

Here, we will explain Sun, Hsieh, and Hwang's scheme without providing perfect forward secrecy.

Sun, Hsieh, and Hwang claimed that the two protocols can provide perfect forward secrecy. However, the second protocol had a secure flaw and it did not provide perfect forward secrecy. Suppose that A's secret key and password are disclosed. First, the attacker can decrypt the $Enc_{Pk_{pwd}}(y)$ with A's password to gain the random number y. Second, the attacker can decrypt $Enc_{PK_A}(r)$ with $A's$ secret key to gain $r = g^x \bmod p$. Then, the attacker computes the decryption key $k = r^y = (g^x)^y \bmod p$. Finally, message M can be decrypted by using the decryption key k.

For example, sender Bob communicates with receiver Alice by performing the secure protocol without using a smart card after having communicated five times already. Suppose that attacker David wants to know the content of the message, he intercepts all the messages communicated by Alice and Bob. Due to David without Alice's secret key and password, he can not gain the transmitted message. However, if David gets Alice's secret key and password, he not only can decrypt the transmitted message in this session but also can decrypt the messages he collected before. Therefore, Sun, Hsieh, and Hwang's second protocol can not satisfy the property of the perfect forward secrecy.

3 Proposed Scheme

From the previous section, we can know that Sun, Hsieh, and Hwang's second protocol cannot provide perfect forward secrecy. Thus, we proposed an improved scheme to achieve the perfect forward secrecy. The details of the improved version are described as follows.

Step 1 (A is off-line): B sends $Enc_{PK_A}(r)$, ID_A, and $Cert$ to mail server.

Step 2 (A is off-line): The mail server sends $g^y \bmod p$ and $Sig_{k_{ms}}(g^y \bmod p)$ to B.

Step 3 (A is off-line): B computes the encryption key $k = (g^y)^x \bmod p$, and encrypts the message using the encryption key k. Next, B sends $E_k(M)$ and $h(k||g^y mod p)$ to the mail server.

Step 4 (B is off-line): A requests mail server for new mails, and mail server asks A to input his ID, original $password$, and his new password $p' = (password \bigoplus r_1)$ to mail server for verification, where r_1 is a random number. If ID and the original $password$ are correct, A can receive new mails. In addition, an old password is replaced by a new password p'. Next, the mail server delivers $Enc_{PK_A}(r)$, $Cert$, $E_k(M)$, $h(k||g^y mod p)$, and $Enc_{Pk_{p'}}(y)$ to A.

Step 5 (B is off-line): After receiving $Enc_{PK_A}(r)$, $Cert$, $E_k(M)$, $h(k||g^y mod p)$, and $Enc_{Pk_{p'}}(y)$, the random number y can be obtained by decrypting $Enc_{Pk_{p'}}(y)$ using his new password p'. And $r = (g^x \ mod \ p)$ can be obtained by decrypting $Enc_{PK_A}(r)$ using A' secret key.

Step 6 (B is off-line): A can compute the decryption key $k = r^y = (g^x)^y \ mod \ p$, and thus message M can be decrypted with the decryption key k.

Basically, Step 1 to Step 3 in ore proposed scheme are the same as that in protocol two [8]. According to the above mentioned improvement, even if $A's$ secret key and original password are known by eavesdroppers, they only can obtain initial message communicated between A and B. Eavesdroppers cannot derive the subsequent message without $A's$ new password. Therefore, the improved scheme can satisfy the property of the perfect forward secrecy.

4 Conclusions

Sun, Hsieh, and Hwang proposed two protocols in 2005, and they claimed that their protocols can provide the perfect forward secrecy. However, in this paper we have already pointed out that the second protocol of their scheme has a secure flaw. In addition, we further proposed an improved scheme to achieve the perfect forward secrecy.

References

[1] A. Bacard, *The Computer Privacy Handbook: A Practical Guide to E-Mail Encryption, Data*

Protection, and PGP Privacy Software. Peachpit Press, 1995.

[2] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, Nov. 1976.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469–672, Apr. 1985.

[4] M. J. H. Lim, M. Negnevitsky, and J. Hartnett, "Personality trait based simulation model of the e-mail system," *International Journal of Network Security*, vol. 3, pp. 172–190, Sept. 2006.

[5] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1977.

[6] B. Schneier, *E-Mail Security with PGP and PEM: How to Keep Your Electronic Mail Private*. John Wiley and Sons, 1995.

[7] C. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[8] H. M. Sun, B. T. Hsieh, and H. J. Hwang, "Secure e-mail protocols providing perfect forward secrecy," *IEEE Communications Letters*, vol. 9, pp. 58–60, Jan. 2005.

[9] X. Tian, R. W. Zhu, and D. S. Wong, "Improved efficient remote user authentication schemes," *International Journal of Network Security*, vol. 4, pp. 149–154, Mar. 2007.

[10] B. Wang and Z. Q. Li, "A forward-secure user authentication scheme with smart cards," *International Journal of Network Security*, vol. 3, pp. 116–119, Sept. 2006.