Journal of Southeast University (English Edition) Vol. 24, No. 2, pp. 139 – 142 June 2008 ISSN 1003—7985

Improvements on robust email protocols with perfect forward secrecy

Jiang Rui Hu Aiqun Yang Xiaohui

(School of Information Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: According to the security shortages of two robust practical email protocols with perfect forward secrecy, attacks on the two protocols are analyzed and corresponding improvements on the two protocols are proposed. First, by analyzing the two email protocols, the corresponding man-in-the-middle attacks are proposed, where the adversary forges the messages in the receiving phase to cheat the two communication participants and makes them share the wrong session keys with him. Consequently, the man-in-the-middle attacks can make the two protocols fail to provide perfect forward secrecy. Secondly, by adding corresponding signatures in the receiving phases of the two protocols, two corresponding improvements on the protocols are proposed to overcome the man-in-the-middle attacks on the two protocols and make them provide perfect forward secrecy. Moreover, the two improved protocols can retain all the merits of the former protocols.

Key words: man-in-the-middle attack; email; network security; perfect forward secrecy

Modern email system has become widely used instead of traditional communication established by pen and paper. It can transfer not only text but also electronic documents, voice, graphics, and financial transactions through the Internet. In order to deliver the email from the sender to the receiver both efficiently and securely, the email system usually employs both conventional and public key cryptographic systems[1-2]. The basic protection in an email system is to encrypt the bulk mail using a conventional cryptosystem with a short-term key and to protect the short-term key using a public-key cryptosystem with the receiver's public key[3-4]. However, this protection cannot provide perfect forward secrecy (PFS) because once the receiver's secret key is disclosed, all the previously used short-term keys will also be opened and hence all the previous emails will be learned. Recently, Kim et al.[5] proposed two practical email protocols[5] providing perfect forward secrecy, which means that the exposure of the sender's or the recipient's long-term secret keys does not compromise previous session keys. The authors claimed that protocol 1 had the advantage that an encryption or a signature algorithm could be implemented using any public key algorithm, and protocol 2 achieved efficiency and perfect forward secrecy simultaneously.

Beginning with the schemes of Sun et al.[6], which cannot really provide the PFS shown by Dent[7], Kim et al. claimed that they improved on the second protocol of Sun et al. and made it really provide PFS by establishing an additional temporary short-term key between an email server and a recipient using the Diffie-Hellman key exchange[8].

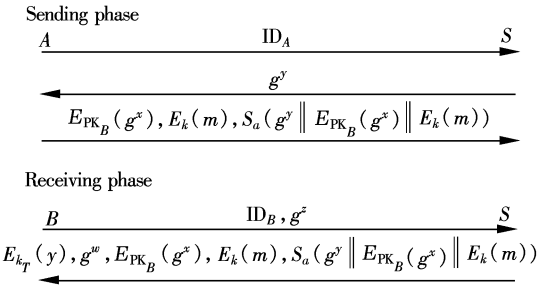
In this paper, we first show that the schemes of Kim et al. can easily suffer from the man-in-the-middle attacks and indeed cannot provide PFS. Then, we propose improvements on two email protocols to avoid such attacks and make them provide PFS and retain all the merits of the former schemes.

1 Review of Schemes Proposed by Kim et al.

The schemes of Kim et al. have two protocols. Protocol 1 is an improved version of the second protocol of Sun et al. and protocol 2 is more efficient than the first one by using a concept of the signcryption of Zheng[9].

1.1 Protocol 1

Protocol 1 has two phases, the sending phase and the receiving phase, which can be shown as follows:



where A, B, S are the sender, the recipient and the email server, respectively; ID_X is the identity of X; PK_X is the public key of X; SK_X is the secret key of X corresponding to PK_X; a, b, s are the signing keys of A, B, S, respectively; k is the session key; t, w, x, y, z, z' are the random numbers; p, q are the large prime numbers; m is the message; $S_s(m)$ is the signature with signing keys on a message m; $E_k(m)$ is the symmetric encryption of a plaintext m using a symmetric key k; $E_{\mathrm{PK}_X}(m)$ is the public encryption of a plaintext m using a public key PK_X; $\|$ represents the concatenation of binary strings.

In the sending phase, when A wants to send an email to B, A sends its identity ID_A to server S. Upon receiving ID_A, S randomly selects y, computes $g^y \bmod p$, and sends it to A. A then randomly chooses x and computes a session key $k = (g^y)^x \bmod p$. A encrypts email contents m with k, $g^x \bmod p$ with PK_B, and signs on $g^y \| E_{\mathrm{PK}_B}(g^x) \| E_k(m)$. Finally, A transmits $E_{\mathrm{PK}_B}(g^x)$, $E_k(m)$, and $S_a(g^y \| E_{\mathrm{PK}_B}(g^x) \| E_k(m))$ to S. Having received the email, S verifies the signature to explicitly authenticate A and stores the email.

In the receiving phase, when B wants to receive the email, B first selects a random number z, computes $g^z \bmod p$, and sends it with ID_B to S. Then S chooses a random number w, computes a temporary short-term key $k_T = (g^z)^w \bmod p$, and encrypts y with k_T. Finally, S sends the email with $E_{k_T}(y)$

Received 2007-10-26.

Biography: Jiang Rui (1968—), male, doctor, associate professor, R. Jiang @seu.edu.cn.

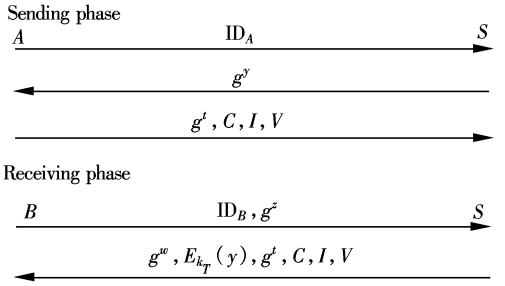
Foundation item: The Natural Science Foundation of Jiangsu Province (No. BK2006108).

Citation: Jiang Rui, Hu Aiqun, Yang Xiaohui. Improvements on robust email protocols with perfect forward secrecy[J]. Journal of Southeast University (English Edition), 2008, 24(2): 139 – 142.

and $g^w \bmod p$ back to B. Having received the encrypted email, B verifies the signature $S_a(g^y \| E_{PK_B}(g^x) \| E_k(m))$ and computes $k_T = (g^w)^z \bmod p$, then decrypts $E_{k_T}(y)$ and $E_{PK_B}(g^x)$ to derive a session key k. Finally, B receives the email from $E_k(m)$ using $k = (g^x)^y \bmod p$.

1.2 Protocol 2

Protocol 2 is more efficient than the second protocol of Sun et al. and protocol 1. It has three phases: the setup phase, the sending phase and the receiving phase. The sending and receiving phases can be shown as follows:



where $U = (PK_B g^y)^x$, $k = PRF(U)$, $k_1 \| k_2 = k$, $C = E_{k_1}(m)$, $I = MAC_{k_2}(m)$, $V = x(t + SK_A)^{-1}$, $MAC_k(m)$ is the message authentication code on m using a secret key k; $PRF(k)$ is the pseudo-random value of k using a pseudo-random function PRF.

In the setup phase, the system parameters (p, q, g) are chosen, where p and q are two large primes satisfying $q \mid (p-1)$, and $g \in \mathbf{Z}_p^*$ is an element of order q. A and B randomly choose SK_A and SK_B, then compute $PK_A = g^{SK_A} \bmod p$ and $PK_B = g^{SK_B} \bmod p$, respectively.

In the sending phase, when A wants to send an email to B, A sends ID_A to S. Upon receiving ID_A, S randomly selects y, computes $g^y \bmod p$, and sends it to A. A randomly chooses x and computes a session key $k = PRF(U)$, where $U = (PK_B g^y)^x \bmod p$. A then splits k into k_1 and k_2. k_1 is used as a conventional encryption key and k_2 is used as a MAC key. A encrypts a message m with k_1, i.e., $C = E_{k_1}(m)$, and computes the MAC with k_2, i.e., $I = MAC_{k_2}(m)$. Finally, A randomly selects t, computes $g^t \bmod p$ and $V = x(t + SK_A)^{-1} \bmod q$, and transmits $g^t \bmod p$, C, I and V to S.

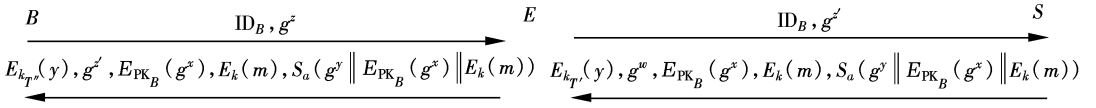
In the receiving phase, when B wants to receive the email, B sends his identity ID_B and $g^z \bmod p$ to S. S randomly chooses w to encrypt y with a short-term key $k_T = (g^z)^w \bmod p$. S finally delivers $g^w \bmod p$ with $E_{k_T}(y)$, g^t, C, I and V to B. B computes $k_T = (g^w)^z \bmod p$, $U = (PK_A g^t)^{V(SK_B + y)} \bmod p$, and $k = PRF(U)$, then splits k into k_1 and k_2 as A did. If $MAC_{k_2}(m)$ is equal to I, B obtains the email contents by decrypting the cipher text C with key k_1, i.e., $m = E_{k_1}^{-1}(C)$.

2 Our Attacks on Protocols of Kim et al.

In this section, we show that the above two protocols easily suffer from the man-in-the-middle attacks, and cannot provide perfect forward secrecy.

2.1 Attack on protocol 1

In the sending phase, the adversary E eavesdrops on the messages sent between A and S. When the receiving phase begins, he can make the man-in-the-middle attack on the protocol, which is shown as follows:



First, the adversary E intercepts the message ID_B, g^z sent by B to S, selects a random number z', computes $g^{z'} \bmod p$, then he replaces $g^z \bmod p$ with $g^{z'} \bmod p$, and sends the changed message ID_B, $g^{z'}$ to S. Upon receiving the message, S will compute a wrong temporary short-term key $k_{T'} = (g^{z'})^w \bmod p$, and encrypt y with $k_{T'}$. Finally, S sends the email with $E_{k_{T'}}(y)$ and g^w back to B.

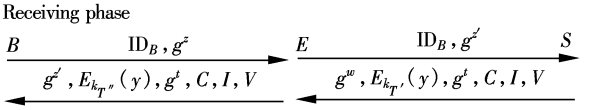
Secondly, the adversary E again intercepts the message sent by S to B, decrypts $E_{k_{T'}}(y)$ to obtain y with the key $k_{T'} = (g^w)^{z'} \bmod p$, then computes $k_{T''} = (g^z)^{z'} \bmod p$, encrypts y with $k_{T''}$, and replaces g^w with $g^{z'}$. Finally, the adversary E sends the email with $E_{k_{T''}}(y)$ and $g^{z'}$ back to B. Having received the encrypted email, B can verify the signature, compute $k_{T''} = (g^{z'})^z \bmod p$, then decrypt $E_{k_{T''}}(y)$ and $E_{PK_B}(g^x)$ to derive session key k. Finally, B can receive the email content m from $E_k(m)$ with the session key $k = (g^x)^y \bmod p$.

Finally, when the protocol finishes, everything seems well to both B and S. However, both S and B do not know they share the wrong temporary short-term key $k_{T'}$ and $k_{T''}$ with the adversary, respectively. More important, the secret number y is disclosed. Unfortunately, both S and B still think they share the common short-term key with each other. This is the typical man-in-the-middle attack.

Moreover, when the recipient's long-term secret key is exposed, i.e., SK_B is exposed, the adversary can easily obtain g^x from $E_{PK_B}(g^x)$, and compute session key $k = (g^x)^y \bmod p$ (because he obtained the secret y earlier). Thus, the session key k is disclosed. Therefore, protocol 1 cannot provide perfect forward secrecy.

2.2 Attack on protocol 2

Similar to protocol 1, in the sending phase, the adversary E eavesdrops on the messages sent between A and S. When the receiving phase begins, he can make the man-in-the-middle attack on the protocol, which is shown as follows:



First, the adversary E intercepts the message ID_B, g^z sent by B to S, selects a random number z', computes $g^{z'} \bmod p$, then he replaces $g^z \bmod p$ with $g^{z'} \bmod p$, and sends the changed message ID_B, $g^{z'}$ to S.

Secondly, when S sends the encrypted email back to B, the adversary E again intercepts the message, gets the secret y, replaces $E_{k_{T'}}(y)$ with $E_{k_{T''}}(y)$, where $k_{T'} = (g^w)^{z'} \bmod p$ and $k_{T''} = (g^z)^{z'} \bmod p$, replaces g^w with $g^{z'}$, and sends the changed message $g^{z'}$, $E_{k_{T''}}(y)$, g^t, C, I, V to B. Having received the encrypted email, B can verify $\mathrm{MAC}_{k_2}(m)$ and finish the protocol successfully, and he cannot know what has happened. Actually, both S and B share the wrong temporary short-term key $k_{T'}$ and $k_{T''}$ with the adversary, respectively. Therefore, protocol 2 suffers from the man-in-the-middle attack.

Also, the secret y is disclosed to the adversary. Once the recipient's long-term secret key is exposed, i. e., SK_B is exposed, the adversary can compute U as follows:

$$(\mathrm{PK}_A g^t)^{V(\mathrm{SK}_B+y)} \bmod p = (g^{\mathrm{SK}_A+t})^{V(\mathrm{SK}_B+y)} \bmod p = (g^{SK_B+y})^x \bmod p = (\mathrm{PK}_B g^y)^x \bmod p = U$$

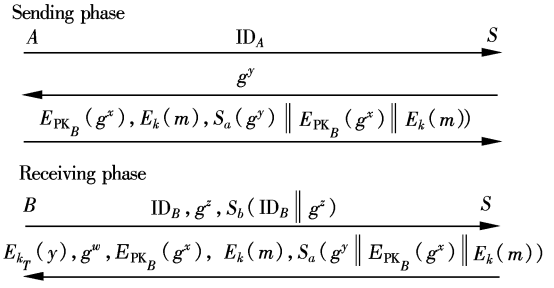
Then, the adversary can compute $k = \mathrm{PRF}(U)$, and the session key k is disclosed. Therefore, protocol 2 also cannot provide perfect forward secrecy.

3 Our Improvements on Two Protocols

In this section, we propose our improvements on two protocols to overcome attacks and provide perfect forward secrecy.

3.1 Improvement on protocol 1

The reason why protocol 1 easily suffers from the man-in-the-middle attack is that the server S cannot authenticate recipient B. The server S cannot distinguish whether the message ID_B, g^z is sent by B or the adversary. So, in order to overcome this kind of attack, we propose our improvement on protocol 1, which is shown as follows:

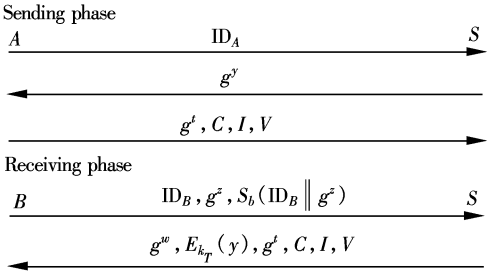


Our improved protocol 1 has two phases, the sending phase and the receiving phase. The sending phase in our advanced protocol 1 is the same as the former protocol 1. In the receiving phase, when B wants to receive the email, B should add his signature in the message, that is, B should send ID_B, g^z, $S_b(\mathrm{ID}_B \| g^z)$ instead of ID_B, g^z to S. Having received this message, S can make sure that the message ID_B, g^z, $S_b(\mathrm{ID}_B \| g^z)$ is sent only by B, according to the verification of the signature $S_b(\mathrm{ID}_B \| g^z)$, since any adversary cannot forge the correct $S_b(\mathrm{ID}_B \| g^z)$. S then sends the message $E_{k_T}(y)$, g^w, $E_{\mathrm{PK}_B}(g^x)$, $E_k(m)$, $S_a(g^y \| E_{\mathrm{PK}_B}(g^x) \| E_k(m))$ back to B, and finally B receives the email from $E_k(m)$ using $k = (g^x)^y \bmod p$.

When an adversary wants to replace $g^z \bmod p$ with $g^{z'} \bmod p$ as he does in our attack 1, he cannot calculate the correct $S_b(\mathrm{ID}_B \| g^{z'})$, because he does not know the signing key b of the recipient B. Thus, the server S will easily find out the forged message and reject it; therefore, the above man-in-the-middle attack 1 can be avoided, and the secret number y can be protected. So, even if the long-term secret keys SK_A and SK_B are exposed to an adversary, computing $k = (g^x)^y \bmod p$ is infeasible without y under the hardness assumption of the Diffie-Hellman problem. Therefore, our improved protocol 1 can provide PFS. It is also obvious that our improved protocol 1 can retain the merits of the former protocol 1.

3.2 Improvement on protocol 2

Similar to protocol 1, the reason why protocol 2 easily suffers from the man-in-the-middle attack is that the server S also cannot authenticate the recipient B. So, in order to overcome this kind of attack, we propose our improvement on protocol 2, which is shown as follows:



Our improved protocol 2 has three phases: the setup phase, the sending phase and the receiving phase. The setup phase and the sending phase in our advanced protocol 2 are the same as that of the former protocol 2. In the receiving phase, when B wants to receive the email, B should add his signature in the message, that is, B should send ID_B, g^z, $S_b(\mathrm{ID}_B \| g^z)$ instead of ID_B, g^z to S. Having received this message, S can make sure the message ID_B, g^z, $S_b(\mathrm{ID}_B \| g^z)$ is sent only by B, according to the verification of the signature $S_b(\mathrm{ID}_B \| g^z)$, since no adversary can forge the correct $S_b(\mathrm{ID}_B \| g^z)$. S then sends the message g^w, $E_{k_T}(y)$, g^t, C, I, V, and finally B obtains the email contents by decrypting the cipher text C with key k_1.

When an adversary wants to replace $g^z \bmod p$ with $g^{z'} \bmod p$ as he does in our attack 2, he cannot calculate the correct $S_b(\mathrm{ID}_B \| g^{z'})$, because he does not know the signing key b of the recipient B. Thus, the server S will easily discover the forged message and reject it, therefore the above man-in-the-middle attack 2 can be avoided, and the secret number y can be protected. Although an adversary gets all long-term secret keys SK_A and SK_B, he cannot compute U due to the fact that y is protected and not exposed. Therefore, our improved protocol 2 can provide PFS. It is also obvious that our improved protocol 2 can retain all the merits of the former protocol 2.

4 Conclusion

In this paper, we first propose the man-in-the-middle attacks on two protocols of Kim et al. and show the two protocols which cannot provide perfect forward secrecy. Then, we propose our improvements on two protocols to overcome the

man-in-the-middle attacks and make them provide perfect forward secrecy. Also, our two improved protocols can retain all the merits of the former protocols.

References

[1] Schneier B. *Applied cryptography* [M]. 2nd ed. New York: John Wiley & Sons, Inc., 1995: 56 - 120.

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

[3] Schneier B. *Email security*: *how to keep your electronic mail private* [M]. New York: John Wiley & Sons, Inc., 1995: 81 - 156.

[4] Bacard A. *The computer privacy handbook*: *a practical guide to email encryption*, *data protection*, *and PGP privacy software* [M]. Peachpit Press, 1995: 18 - 126.

[5] Kim B, Koo J, Lee D. Robust email protocols with perfect forward secrecy [J]. *IEEE Communications Letters*, 2006, **10**(6): 510 - 512.

[6] Sun H, Hsieh B, Hwang H. Secure email protocols providing perfect forward secrecy [J]. *IEEE Communications Letters*, 2005, **9**(1): 58 - 60.

[7] Dent A W. Flaws in an email protocol of Sun, Hsieh, and Hwang [J]. *IEEE Communications Letters*, 2005, **9**(8): 718 - 719.

[8] Diffie W, Hellman M E. New directions in cryptography [J]. *IEEE Transactions on Information Theory*, 1976, **22**(5): 644 - 654.

[9] Zheng Y. Digital signcryption or how to achieve cost(signature and encryption) [C]//*CRYPTO'* 97. Santa Barbara, California, USA, 1997: 165 - 179.

具有完美前向机密性的鲁棒电子邮件协议的改进

蒋 睿 胡爱群 杨晓辉

(东南大学信息科学与工程学院,南京 210096)

摘要: 针对2个具有完美前向机密性的鲁棒电子邮件协议所存在的安全缺陷,分析了2个协议所面临的协议攻击,并得出了相应的改进方案. 首先,通过对2个电子邮件协议的分析,提出了相应的中间人攻击方法,其中攻击者在协议的接收阶段通过伪造信息来欺骗通信双方,并使通信双方与其共享错误的会话密钥. 由此中间人攻击使得2个电子邮件协议的完美前向机密性得不到保证. 其次,通过在2个协议的接收阶段加入相应的签名信息,提出了对2个协议的改进方案,以确保改进协议能够克服中间人攻击并且提供协议的完美前向机密性. 此外,经改进的协议仍然能够保持原协议的所有优点.

关键词: 中间人攻击;电子邮件;网络安全;完美前向机密性

中图分类号: TP393