International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.11 (2016), pp.335-342
http://dx.doi.org/10.14257/ijmue.2016.11.11.30

A Secure Multi-receivers E-mail Protocol

Baoyuan Kang and Danhui Xu

School of Computer science and software Tianjin polytechnic university, Tianjin, 300387, China
baoyuankang@aliyun.com,mixueren123123@sina.com

Abstract

In open decentralized networks, it is important to make certain data available to only a selected group of users. For example, in a secure e-mail system, a user may send an e-mail to multiple receivers at once. Recently, Chen proposed a secure multicast key protocol for e-mail system based on Chinese Remainder Theorem. They claimed that their protocol provide perfect forward secrecy and ensure confidentiality and authentication. But, in this paper, we show that Chen's protocol suffers from the sender and the e-mail server impersonation attacks and mail content confidentiality attack. Moreover, we give an improvement to Chen's protocol. To contribute a secure multireceiver e-mail protocol, we propose a novel protocol by adopting Lagrange polynomial interpolation. We also discuss the security of the novel multireceiver e-mail protocol. Our protocol provides the perfect forward secrecy and resists unknown key-share attack, replay attack, sender impersonation attack, e-mail server impersonation attack and mail content confidentiality attack.

Keywords*: Cryptography; Secure protocol; Multireceiver e-mail protocol; Security*

1. Introduction

With the rapid development of Internet, e-mail has become an essential communication tool. Unfortunately the basic e-mail protocol does not provide the confidentiality and integrity service. So, the security of e-mail communications is an important issue. Bacard [1] introduced some security requirements in e-mail systems. Since then, several security protocols such as, PGP [2], PEM [3] and S/MIME [4] have been designed to provide confidentiality and authentication of e-mail system. However, these protocols cannot provide perfect forward secrecy [5] because once the secret key of the receiver is disclosed, all previous used short-term keys will also be opened and hence previous e-mail will be learned.

In order to provide perfect forward secrecy, Sun *et al.* [5] proposed two new e-mail protocols. However, in 2006, Dent [6] pointed out Sun *et al.*'s protocols do not provide perfect forward secrecy as claimed. Later, Kim *et al.* [7] proposed an improved version of Sun *et al.*'s protocols to overcome this weakness. But, in 2010, Chang *et al.* [8] showed that Kim *et al.*'s protocols suffer from the well-known man-the-middle attack and consequently do not achieve perfect forward secrecy. In2007, Kwon *et al.* [11] proposed a password-based e-mail protocol for mobile devices. However too many modular exponentiation operations in their protocol might cause mobile devices consume battery power expeditiously [8].

In open decentralized networks, sometimes, it is necessary to make certain data available to a selected group of users. Such as, in some secure e-mail system, a user may send an e-mail to multiple receivers at once. In order to keep the e-mail content secrecy, the user can encrypt the content by the deployment of multireceiver encryption protocol. Multireceiver encryption schemes can be used in pay-TV [12] secure broadcasting and digital copyright protection [13] biometric authentication privacy [14] and e-mail system.

ISSN: 1975-0080 IJMUE

Recently, Chen [9] and Zhang *et al.* [10] put forward the multireceiver e-mail protocols. Chen proposed a secure multicast key protocol for e-mail system based on Chinese Remainder Theorem. They claimed that their protocol ensure confidentiality and authentication and provide perfect forward secrecy, resist sender impersonation attack, e-mail server impersonation attack, replay attack, unknown key-share attack, forgery attack. But, in this paper, we show that Chen's protocol suffers from the sender and the e-mail server impersonation attacks and mail content confidentiality attack. A secure e-mail protocol must provide the security of mail content confidentiality. But in Chen's protocol the attacker can obtain the mail content by intercepting transmitted messages. Moreover, we give an improvement to Chen's protocol. To contribute a secure multireceiver e-mail protocol, we propose a novel protocol. The design of novel protocol is inspired by the anonymous conference protocol [16]. We also discuss the security of the novel multireceiver e-mail protocol. Our protocol provides the perfect forward secrecy and resists unknown key-share attack, replay attack, sender impersonation attack, e-mail server impersonation attack and mail content confidentiality attack.

This article is organized as follows. We review Chen's protocol in Section 2 and point out its flaws in Section 3. In Section 4, we give an improvement of Chen's protocol. Moreover, we propose a novel multireceiver e-mail protocol in Section 5. The security analysis of the proposed protocol is discussed in Section 6. Finally, conclusions are given in Section 7.

2. Review of Chen's Secure Multireceivers E-mail Protocol

In this section, we review Chen's multireceivers e-mail protocol [9]. Chen's protocol consists of three phases: precomputation, sending and receiving. In the e-mail system, S indicates the mail server, and each user U_i has a pair public key PK_i and secret key SK_i. ID_i, which is a uniquely prime number, indicates the identification of the user U_i.

Precomputation

Step 1. $U_i \to S$: e_i, $Sig_{SK_i}(e_i)$, ID_i.

A user U_i generates another pair of public key and secret key (e_i, d_i), where $e_i \cdot d_i = 1 \bmod \varphi(ID_i)$. This pair of public key and secret key is not related to the pair of public key PK_i and secret key SK_i pre-distributed by the system. The user U_i sends e_i and signature $Sig_{SK_i}(e_i)$ to the e-mail server. Note that this procedure is executed after the user U_i finished receiving an e-mail.

Sending phase

Assume that the sender U_1 intends to send an e-mail to the receivers $U_2, U_3, ..., U_z$. M is the e-mail content. The sender U_1 and e-mail server S execute the following procedures:

Step 2. $S \to U_1$: $e_2, e_3, ..., e_z$; $Sig_{SK_2}(e_2)$, $Sig_{SK_3}(e_3)$,…, $Sig_{SK_n}(e_z)$; $ID_2, ID_3, ..., ID_z$.

Step 3. The sender U_1 chooses two random primes p and q. Next, the U_1 computes $n = p \times q$. Then, he computes another pair of a public key $\hat{e}_s$ and the corresponding secret key $\hat{d}_s$, where $\hat{e}_s \times \hat{d}_s \equiv 1 \bmod \varphi(n)$.

Step 4. Then, the U_1 computes

$$X = \sum_{i=1}^{z} \left(L / ID_i \right) \times \left(\hat{d}_s \right)^{e_i} \times h_i \bmod L$$

Where $L = ID_1 \times ID_2 \times ... \times ID_z$ and $\left(L / ID_i \right) \times h_i = 1 \bmod ID_i$.

Step 5. $U_1 \rightarrow S : X, L, V, W, Y, t, n$ where $V = \hat{d}_s^{\hat{e}_s} \bmod n$, $W = M^{\hat{e}_s} \bmod n$, and $Y = Sig_{PK_1}\left(h\left(ID_1 \| ID_2 \| \cdots \| ID_z \| M \| t \right) \right)$. The parameter t is a timestamp at that time.

Receiving phase

When the receiver U_r connects to his mail server, where $r \in [2,...,z]$, he sends a request for asking new e-mails. Then, the following procedures are executed:

Step 6. $S \rightarrow U_r : X, L, V, W, Y, t, n, ID_1, ID_2, ..., ID_z$.

Step 7. Receiver U_r derives the value $\hat{d}_s' \left(\bmod ID_r \right)$ by computing $\hat{d}_s = X^{d_r} (\bmod ID_r)$. Then, the receiver U_r check if $\left(V \right)^{\hat{d}_s'} \bmod n$ equals to the value $\hat{d}_s'$. If it does, the receiver U_r computes the content $M' = \left(W \right)^{\hat{d}_s'} \bmod n$.Upon deriving the content M', the receiver U_r computes the value $Y' = Sig_{PK_1}\left(h\left(ID_1 \| ID_2 \| \cdots \| ID_z \| M' \| t \right) \right)$ and checks if Y' equals to the value in the signature Y.

3. The Weaknesses of Chen's Protocol

3.1. The Sender and the E-Mail Server Impersonation Attacks

When U_1 wants to send an e-mail to users $U_2, U_3, ...,$ and U_z, the mail server S sends $e_2, e_3, ..., e_z$; $Sig_{SK_2}\left(e_2 \right)$, $Sig_{SK_3}\left(e_3 \right)$, …, $Sig_{SK_n}\left(e_z \right)$; $ID_2, ID_3, ..., ID_z$ to U_1. At this time, an attacker E intercepts the message. Then, E can do following step 3, step 4 and step 5 in Chen's protocol. The attacker E can success in impersonating the sender U_1 attack, because only the public key and ID_1, the identification of the sender U_1 are needed in step 3, step 4 and step 5 in Chen's protocol.

Similarly, the e-mail server can also do this impersonation attack.

3.2. Mail Content Confidentiality Attack

First of all, a secure e-mail protocol should provide the security of mail content confidentiality. That is to say, the mail content cannot be known by anyone else but the intended recipient. But, in Chen's protocol, the identification ID_i of the user U_i is a prime number, when an attacker intercepts the message $e_2, e_3, ..., e_z$; $Sig_{SK_2}\left(e_2 \right), Sig_{SK_3}\left(e_3 \right), \ldots, Sig_{SK_n}\left(e_z \right)$; $ID_2, ID_3, ..., ID_z$ in step 2 in Chen's protocol, the attacker can compute $\varphi(ID_2) = ID_2 - 1$. Then the attacker can compute d_2 by the relation equation $e_2 d_2 = 1 \bmod (\varphi(ID_2)$. So, when the attacker intercepts the message

$X, L, V, W, Y, t, n, ID_1, ID_2, ..., ID_z$ in step 6, the attacker can execute step 7 in Chen's protocol, and obtain the mail content M.

4. The Improved Protocol

Author names and affiliations are to be centered beneath the title and printed in Times New Roman 12-point, non-boldface type. Multiple authors may be shown in a two or three-column format, with their affiliations below their respective names. Affiliations are centered below each author name, italicized, not bold. Include e-mail addresses if possible. Follow the author information by two blank lines before main text.

To improve Chen's protocol, we firstly selects primes numbers p_i and q_i to change the identification ID_i of the user U_i. Let $ID_i = p_i \times q_i$ and keep $ID_1, ID_2, ..., ID_z$ pair-wise relatively primes. Such, the conditions of the Chinese Reminder theorem are also satisfied, and the equation $\hat{d}_s = X^{d_r} (\mathrm{mod}\, ID_r)$ also holds.

But the attacker cannot computes d_r using intercepted e_r, since the attacker cannot compute $\varphi(ID_r)$ under unknowing p_r and q_r. Unknowing d_r, the attacker cannot compute $\hat{d}_s{}'$ and the message M.

Secondly we can replace the equation $Y = Sig_{PK_1}\left(h\left(ID_1 \| ID_2 \| \cdots \| ID_z \| M \| t\right)\right)$ in step 5 in Chen's protocol by the equation

$$Y = Sig_{SK_1}\left(h\left(X \| L \| V \| W \| ID_1 \| ID_2 \| \cdots \| ID_z \| M \| t \| n\right)\right).$$

And in step 7, U_r first verifies the signature

$$Y = Sig_{SK_1}\left(h\left(X \| L \| V \| W \| ID_1 \| ID_2 \| \cdots \| ID_z \| M \| t \| n\right)\right).$$

If this signature is valid, U_r do other computation in step 7 in Chen's protocol.

This improvement can resist the sender and the e-mail server impersonation attack and mail content exposure attack.

5. The Proposed Multireceive E-Mail Protocol

Inspiring by the anonymous conference protocol [16], we propose a novel multireceivers e-mail protocol. The proposed protocol consists of three phases: precomputation, sending and receiving. In the e-mail system, S indicates the mail server, and each user U_i has a pair public key PK_i and secret key SK_i. ID_i indicates the identification of the user U_i, Let $H(\cdot)$ is a collision-resistance hash function, and G_1 be a cyclic additive group generated by P, whose order is a prime q.

Precomputation

Step 1. $U_i \rightarrow S$: $Q_i, Sig_{SK_i}\left(Q_i\right)$, ID_i.

A user U_i selects $x_i \in Z_q^*$ and generates $Q_i = x_i P$. Then he sends Q_i and signature $Sig_{SK_i}\left(Q_i\right)$ to the e-mail server. Note that this procedure is executed after the user U_i finished receiving an e-mail. Also U_i must use a smart card to store x_i

Sending phase

Assume that the sender U_1 intends to send an e-mail to the receivers $U_2, U_3, ...,$ and U_n. The sender U_1 and e-mail server S execute the following procedures:

Step 2. $S \rightarrow U_1$: $Q_2, Q_3, ..., Q_n$; $Sig_{SK_2}(Q_2)$, $Sig_{SK_3}(Q_3)$,…, $Sig_{SK_n}(Q_n)$; $ID_2, ID_3, ..., ID_n$.

Step 3. Let $M \in Z_q^*$ be the message content to be sent. If the $n-1$ signatures are valid, the sender U_1 computes

$k_{1i} = x_1 Q_i$, $h_i = H(k_{1i} \| ID_1 \| ID_i \| T)$, $w = H(M \| ID_1 \| T)$

Where T is time stamp. Then, U_1 constructs a polynomial with degree $n-1$ using n points $(h_i, H(h_i))$ $(i = 2,3,\cdots,n)$ and $(0, M)$ by adopting Lagrange polynomial interpolation as follows

$$F(x) = M \prod_{j=2}^{n} \frac{x - h_j}{0 - h_j} + \sum_{i=2}^{n} H(h_i) L_i(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_1 x + b_0 .$$

Where $L_i(x) = \dfrac{x-0}{h_i - 0} \prod_{j=2, j \neq i}^{n} \dfrac{x - h_j}{h_i - h_j}$. In fact, $b_0 = M$.

Step 4. $U_1 \rightarrow S : I = \{w, T, b_{n-1}, b_{n-2}, \cdots, b_1, Q_1, ID_1, ID_2, \cdots ID_n\}$, $Y = Sig_{SK_1}(I)$.

Receiving phase

When the receiver U_i connects to his mail server, where $i \in [2, ..., n]$, he sends a request for asking new e-mails. Then, the following procedures are executed:

Step 5. $S \rightarrow U_i : I = \{w, T, b_{n-1}, b_{n-2}, \cdots, b_1, Q_1, ID_1, ID_2, \cdots ID_n\}$, $Y = Sig_{SK_1}(I)$

Step 6. Receiver U_i verifies the signature $Y = Sig_{SK_1}(I)$. If it does, U_i computes $k_{i1} = x_i Q_1$, $h_i = H(k_{i1} \| ID_1 \| ID_i \| T)$,

$M' = H(h_i) - b_{n-1} h_i^{n-1} - b_{n-2} h_i^{n-2} - \cdots b_1 h_i$. And checks if $w = H(M' \| ID_1 \| T)$.

6. Security Analysis of the Proposed Protocol

6.1. Perfect Forward Secrecy

In a protocol, if compromise of long-term keys does not compromise session keys, it's said that the protocol satisfies the perfect forward secrecy. In our protocol, the session key k_{1i} is determined by the randomly selected secret numbers x_1 and x_i . So, the session key k_{1i} has no relationship with the long-term SK_1 or SK_i . Therefore, compromise of long-term keys does not compromise session keys. Our protocol satisfies the perfect forward secrecy.

6.2. Unknown Key-Share Attack

The unknown key-share attack can be considered as a special case of impersonation attacks. It can cheat a victim user to construct a short-term with the adversary, whom the victim user thinks as an authorized user and sends message to him. In our protocol, in step 2 the Q_i is sent with its signature $Sig_{SK_i}(Q_i)$, in step 5 the Q_1 is sent with signature $Sig_{SK_i}(I)$, Q_1 is included in I . So, the messages in step 2 and step 5 can be check. Moreover, the session key k_{1i} is related to Q_1 and Q_i , So the adversary cannot construct a short-term with the a victim user.

6.3. Replay Attack

An adversary may intercept massage in step 1, step 2, step 4 and step 5. But in our protocol the Q_i of user U_i is renewed when each receiving e-mail is finished. Secondly, time stamp T is involved in step 3, step 4 and step 5 to guarantee the freshness of transmitted messages. So, the intercepted message are useless for the adversary to make replay attacks.

6.4. Sender Impersonation Attack

An adversary wants to impersonate user U_1 to send a message to users $U_2, U_3 \cdots, U_n$, he must know secret number x_1 and private key SK_1. Because in step 3 x_1 is needed while computing k_{1i} and in step 4 SK_1 is needed to compute the signature. The adversary do not know SK_1 and x_1, and x_1 is often renewed. So, the adversary cannot success to do sender impersonation attack.

6.5. E-Mail Server Impersonation Attack

In our protocol the e-mail server only play a role that relays the message sent by the sender. So, it is meaningless for an adversary to impersonate a legitimate e-mail server to send message to receivers.

6.6. Mail Content Confidentiality Attack

Unlike Chen's protocol, our protocol can resist mail content confidentiality attack. An adversary may intercept w in step 4, but, at first the mail content M is protected by the hash H. Secondly, Except $U_2, U_3 \cdots U_n$, nobody can compute k_{i1}, So, anyone out of the intended receivers group can obtain the mail content M through computation in step 6.

7. Conclusion

In this paper, we show that Chen's protocol suffers from the sender and the e-mail server impersonation attacks and mail content confidentiality attack. Moreover, we give an improvement to Chen's protocol. To contribute a secure multireceiver e-mail protocol, we propose a novel protocol by adopting Lagrange polynomial interpolation. We also discuss the security of the novel multireceiver e-mail protocol. Our protocol provides the perfect forward secrecy and resists unknown key-share attack, replay attack, sender impersonation attack, e-mail server impersonation attack and mail content confidentiality attack.

Acknowledgements

This work is supported by the Applied Basic and Advanced Technology Research Programs of Tianjin (No. 15JCYBJC15900).

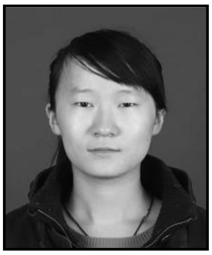
References

[1] A. Bacard, "Computer Privacy Handbook: A Practical Guide to e-mail Encryption, Data Protection, and PGP Privacy Software", Berkeley, CA: Peachpit Press, **(1995)**.
[2] D. Atkins, W. Stallings and P. Zimmermann, "PGP Message Exchange Formats", Internet Draft, **(1995)**.
[3] D. Balenson, "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", RFC, pp. 1423, 1993.
[4] J. Galvin, G. Murphy, S. Crocker and N. Freed, "MIME Object Security Services", RFC, pp. 1848, 1995.

[5] H. Sun, B. Hsieh and H. Hwang, “Secure e-mail protocols providing perfect forward secrecy”, IEEE Communications Letters, vol. 15, no. 8, **(2005)**, pp. 58-60.
[6] A. W. Dent, “Flaws in an e-mail protocol of Sun, Hsieh, and Hwang”, IEEE Communications Letters, vol. 9, no. 8, **(2005)**, pp. 718-719.
[7] B. Kim, J. Koo and D. Lee, “Robust e-mail protocols with perfect forward secrecy”, IEEE Communications Letters, vol. 10, no. 6, **(2006)**, pp. 510-512.
[8] C. Chang, C. Lee and Y. Chiu, “An efficient e-mail protocol providing perfect forward secrecy for mobile devices”, International Journal of Communication Systems, vol. 23, **(2010)**, pp. 1463-1473.
[9] C. Chen, “Secure multicast key protocol for electronic mail systems with providing perfect forward secrecy”, Security and Communication Network, vol. 6, **(2013)**, pp. 100-107.
[10] M. Zhang and T. Takagi, “Efficient Constructions of Anonymous Multireceiver Encryption Protocol and Their Deployment in Group E-mail Systems With Privacy Preservation”, IEEE Systems Journal, vol. 7, no. 3, **(2013)**, pp. 410-419.
[11] J. O. Kwon, I. R. Jeong, K. Sakurai and D. H. Lee, “An efficient password-based e-mail protocol for encrypted e-mail transmissions on mobile equipment”, Proceedings of the 2007 IEEE International Conference on Consumer electronics (ICCE 2007), Las Vegas, U.S.A., **(2007)**, pp. 2–22, 1–2.
[12] A. Narayanan, C. Rangan and K. Kim, “Practical pay TV schemes”, in proc. ACISP, LNCS 2727, **(2003)**, pp. 192-203.
[13] S. C. Seshadri and D. Chourishi, “Secure content sharing using third party with broadcast encryption for stateless receivers”, in Proc. IEEE Int. Conf. Computer Science Information Technology, **(2009)**, pp. 528-531.
[14] H. M. Lu, F. Bui, N. Plataniotis and D. Hatzinakos, “A biometric encryption system for the self-exclusion scenario of face recognition”, IEEE Syst. J., vol. 3, no.4, **(2009)**, pp. 440-450.
[15] B. K. Schneier, “A chosen ciphertext attack against several e-mail encryption protocols”, in Proceeding SSYM, **(2000)**, pp. 18.
[16] W. Kim, E. Ryu and J. Yoo, “New conference key agreement protocol with user anonymity”, Computer Standards and Interfaces, vol. 27, **(2005)**, pp. 185-190.

Authors

Baoyuan Kang, Received M.S. in algebra from the shanxi University, and Ph.D. in cryptography from Xidian University, People’s Republic of China in 1993 and 1999, respectively. From 1993 to 1999, he taught mathematics in Northwestern Polytechnic University. Since 1999 he has taught mathematics and computer science in Central South University. Now he is a professor at Tianjin Polytechnic University. His current research interests are cryptography and information security.



Danhui Xu, received B.S. in Computer Science from the Tianjin Polytechnic University, China in 2013. Now he is a postgraduate student at Tianjin Polytechnic University. His current research interests are cryptography and information security.