2012 International Conference on Image, Vision and Computing (ICIVC 2012)
IPCSIT vol. 50 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V50.52

Identity-Based Cryptosystem Secure E-mail System

Yan Shi-Jia[1+] and Wei Lan[2]

[1]Computer Department, Sichuan University, Chengdu, China
[2]Software Engineering, Sichuan University, Chengdu, China

Abstract. To solve the key distribution problems in the IBC scheme, this paper proposes a new key distribution protocol based on HIBE key distribution protocol and part of keys manage, which improves the IBC scheme. A new secure E-mail scheme based on Identity-Based Cryptosystems is designed with the combination of GDH group signatures and key manage protocols. It ensures not only the confidentiality, integrity and authenticity, but also the non-repudiation and tracing of the e-mail owing to the improved PKG. The new scheme is compatible with the existing mail protocols and has some practicability as well as application prospects.

Keywords: Identity-Based Cryptosystem; HIBE; GDH group signature; secure E-mail.

1. Introduction

With the rapid development and popularization of Internet, e-mail with convenient and fast characteristics has become the main information transmission tool on the Internet. However, in the most of the current e-mail systems, encryption and authentication mechanisms of e-mail are relatively simple, which lack of effective security protection mechanisms, that make the development of e-mail has faced with intercepted the message by malicious attackers , sender fraud of passing off identity message of others, spam and other security problems.

The currently more mature programs or standards [1] of e-mail that solve the security issue of e-mail are PGP, PEM, S / MIME and so on. These programs are based on public key infrastructure PKI.

To reduce the overhead of public key certificate management, Shamir proposed identity-based cryptography (IBC) [2-3] in 1984. In this public key cryptosystem, the public key can be any of a string. Usually it is the user’s publicly available identifiers, and the user’s public key can be based on these open identity calculated without having to get through the public key certificate. Private-key pass through a third trusted authority TA (Trusted Authority) based on the public key to generate and sent to the user.

There is an important difference in IBC programs and PKI program: In program of PKI, to ensure that only the recipient can read the letter the recipient is the sender’s certificate are based on the recipient’s public key and encrypted with the public letter, in other words, to ensure that the identity of the recipient task is the sender to do. In the IBC program, to ensure that the identity of the recipient task is the recipient themselves, that the recipient access to decryption keys are required for the trusted third party to prove their identity.

This distinction embody superior of the IBC program:

- When the recipient to update their certificate every time, the sender does not need to re-obtain the recipient’s public key.
- Even if the recipient has not set up own public key, the sender can give letter to the recipient.

Corresponding author. Tel.: +15208210850.
E-mail address: ysj58421@126.com.

- Because the keys are generated as required the involvement of trusted third party, the sender can make some limited conditions to received the letter. It sends the secret key to the recipient only when the conditions for recognition set up by a trusted third party.

2. IBC-based Secure Email

The program based on IBC's secure email scheme only solve the issue of confidentiality, and lack of integrity and authenticity, and there is also a security risk in private key distribution process of users. To solve this problem, we design a new security IBC -based email solution IBC-New Email.

2.1. Analysis of Secure E-mail Program

2.1.1. Secure Key Distribution Protocol

For e-mail system based on IBC, PKG how to generate and distribute securely the user's private key is a difficult problem. This paper proposes a new key distribution protocol based on HIBE [4] key distribution protocol and part of keys manage [5], which make key can be determined by both the user and the center of key distribution. The first assumes that the user is in t layer of program, the user's identity is defined as a tuple. In the hierarchical structure, ancestor of user is the root PKG and low-level PKG, the identity of the underlying PKG is a tuple. Realization process is as follows:

a) First of all, each level PKG will be randomly generate their secret elements $s_i \in Z_q^*(1 \le i \le t-1)$ and then submit $ID_i = (ID_1, ..., ID_i)$ and $s_i^{-1}P_i(P_i = H_1(ID_1 \| ... \| ID_i))$ to the root PKG.

b) Then user randomly selecte $r_{ID} \in Z_q^*$ and submit $(ID_t, r_{ID}^{-1}P_0)$ to the bottom level PKG.

c) PKG will randomly selecte $x \in Z_q^*$, and calculate $W = s_{t-1}H_1(ID_t)$, then send to users.

d) When the user received W , then he will get the part of private key $d_{id}^t = s_{t-1}H_1(ID_t)$, and send the tuple $(H_1(ID_t), P_{t-1}, r_{ID}d_{id}^t, r_{ID}P_t)$ to the root PKG.

e) Root PKG receive (m, n, o, p) , inquire database of itself to extract the tuple $(ID_1, ..., ID_{t-1}, P_{t-1}, s_{t-1}^{-1}P_{t-1})$ which is consistent with $P_{t-1} = n$. Then, it need judge the equation $e(o, s_{t-1}^{-1}P_{t-1}) \equiv e(m, p)$ to authenticate whether the user is legitimate. If he is legitimate, the PKG will give key $S_{t+1} = \sum_{i=2}^{t+1} s_{i-1}P_i$ to user.

f) After the user received S_{t+1} , he conjuncte with themself private key $r_{ID}P_t$, and get the final private key $d_{ID} = S_{t+1} + r_{ID}P_t$.

2.1.2. ID-based Signature Scheme

To ensure authenticity and integrity of message, we use the GDH-based group [6-7] as the signature on the mail system to improve the program. Realization process is as follows:

Using Security key distribution protocol, it finish the consultation of the session key agreement between the sender and PKG, using the session key to encrypt identity information and password and request the PKG to authenticate the identity. When validation is complete, PKG will sent the sender's private key which is encrypted by the session key passed to the sender. Sender signatures the e-mail and encrypts message by the recipient's public key, at the same time, generates a summary of the message body which together with the message header, message body and signature to recipient. Recipient uses the same manner to finish the consultation with the PKG and obtains the recipient's private key. Recipient authenticates the sender's signature and re-calculates a summary of the message body, and comprises them, if they are same, indicating that the message has not been tampered with, otherwise e-mail has been tampered with.

2.2. IBC-NewEmail Design

In the IBC-New Email, the process of mail handing includes sending, receiving and verification. Figure 1 describes the process of sending and receiving.

Defined as follows:

Sender: Sender mail domain, *Receiver:* Receive e-mail domain, *M:* plain text message body, *C:* ciphertext message, *IDA*: user A's identity, the paper refers to the A's e-mail address, *PsdA*: A user password corresponding to IDA, *Session A* : A conversation with the PKG, *Session B* : B conversation with the PKG, *Ek(X):* k on X using the symmetric key encryption, *Email-ID:* e-mail ID, *H (X):* calculate the hash value of X, *s • X:* integer s and elliptic curves multiplied by the point X, *Sigk(X):* k on X with the private key signature.

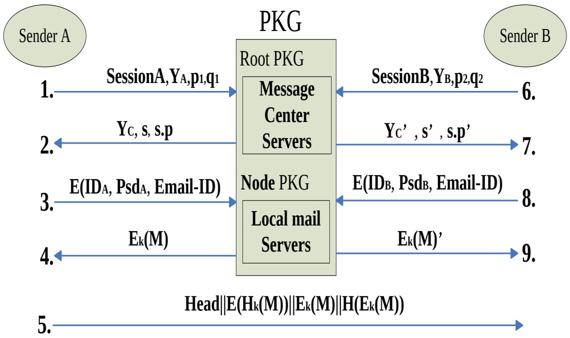

Fig. 1 The process of sending and receiving e-mail

2.2.1. Send E-mail

SenderA → PKG: A prepares the message M, the package is ready to send. A generates prime p_1 and it's origin root q_1 and then generate a random integer R_{A_1} and calculate $Y_{A_1} = q_1^{R_{A_1}} \bmod p_1$ .A randomly generates string SessionA as this session and sends SessionA , Y_{A_1} , p_1 , q_1 to the PKG.

PKG → SenderA: The PKG response Sender A's request, and record this session, and then generate a random integer R_{C_1} , computing $Y_{C_1} = q_1^{R_{C_1}} \bmod p_1$, $K_1 = (Y_{C_1})^{R_{C_1}} \bmod p_1$, and then sent Y_{C_1} and the related public parameters of the IBC S , $S \cdot P$ to the A.

Sender A → PKG: First of all, Sender A will get tuple $(Y_{C_1}, S, S \cdot P)$ and then calculate $K_1 = (Y_{C_1})^{R_{A_1}} \bmod p_1$. Last, A send $E_{K_1}(ID_A \| Psd_A \| Email\_ID)$ to the PKG.

PKG → Sender A: After the PKG accept the request of A, they will make the decryption information $D_{K_1}(E_{K_1}(ID_A \| Psd_A \| Email\_ID))$ which is used to determine Sender A identity of legitimacy. If Sender A is legal, the PKG will give part of the key S_{t+1} to A, while Email_ID be saved. Sender A combines key which is ifself to get the final key d_{ID} .

SenderA → ReceiverB: First of all, Sender A sends $Head \| Sig_{K_A}(H(M)) \| E_{K_A}(d_{ID}) \| H(C)(C = E(M))$ to B, and then destructs this session.

2.2.2. Receive E-mail

Receiver B → PKG: B requests the private key for the PKG. B generates prime p_2 and it's origin root q_2 , and then generates a random integer R_{B_1} and calculates $Y_{B_1} = q_2^{R_B} \bmod p_2$. B randomly generates SessionB as this session and sends SessionB, Y_{B_1} , p_2 and q_2 to the PKG.

PKG → Sender B: PKG will response Sender B's request and record this session, and then generate a random integer R_{C_2} , at the same time, compute $Y_{C_2} = q_2^{R_{C_2}} \bmod p_2$ and $K_2 = (Y_{C_2})^{R_{C_2}} \bmod p_2$, last sent Y_{C_2} and the related public parameters S' , $S' \cdot P'$ of IBC to B.

SenderB → PKG: First of all, Sender B will get $(Y_{C_2}, S', S' \cdot P')$ and calculate $K_2 = (Y_{C_2})^{R_{B_1}} \bmod p_2$, and then send $E_{K_2}(ID_B \| Psd_B \| Email\_ID)$ to the PKG.

PKG → Sender A: After the PKG get the request of B, it will need decrypt the identity information $D_{K_2}(E_{K_2}(ID_B \| Psd_B \| Email\_ID))$ of B to determine the legality of Sender B. If the Sender B is legitimate, the PKG will be give part of the key S_{t+1}' to B, while be saved Email_ID. B use itself key to get the final key d_{ID}' .

SenderB → PKG: When Receiver B receives d_{ID}', will send a confirmation message which include SessionB and Email_ID to the PKG.

Receiver B uses d_{ID}' to decrypt $D_{K_2}(E_{K_2}(k))$ and get k, and then uses k to decrypt the received message body M.

2.2.3. Authentication E-mail

First authenticate whether messages have been tampered with in the half-way, in other words, authenticate message integrity, calculating $H(E_k(M))$ is equal to $H(C)$, if equal that message has not been tampered with, if not equal to abandon the message, otherwise decrypt the received e-mail, accessing M. For verifying the correctness of the message signature, Receiver B decrypts the signature and compares $H'(M)$ with $H(M)$, if they are same, the signature is legal, otherwise that the message is tampered or illegal signature, that does not receive mail.

3. Program Analysis

3.1. Security Analysis

IBC-New Email is the improvement of IBC Scheme. Therefore, the confidentiality of messages can be effectively guaranteed. We only need analysis the IBC-New Email improvements and new features for security.

3.1.1. The Security of Key Distribution

IBC-New Email which based on the original IBC program design the new key management which based on HIBE and part of the key distribution protocol. The HIBE key distribution protocol and the key management protocol themselves can resist a variety of attacks, then IBC-New Email can prevent fraud and eavesdropping, thus ensuring the secure distribution of keys, which makes e-mail confidentiality has been further strengthened.

3.1.2. Authenticity and Integrity

In verification process of the e-mail, Receiver B vivificates Sender A’s signature, and re-calculates a summary of the message body, and be comprised with the original summary of message, if they are same, indicating that the message had not been tampered with, then the receiving mail, if different, that e-mail has been tampered with, then the message is not received. The above process can not only ensure the confidentiality of the message, but also to ensure the integrity of the message.

3.2. Extended Analysis

This program can be extended to any level to form a scalable identity-based e-mail system. The purpose of hierarchical expansion has the three, first, in order to reduce the risk that reduce bottlenecks, making even if there is a problem be caused by a node, it only affects users of the node and will not affect other users. Second, the task is to reduce the assignments of the central node, so that sub-root layer nodes can share some task of root node. The third is to achieve non-repudiation and e-mail traceability.

- After expanding in the program, the root node make some tasks which confirm the identity of users delegate to the domain node, the central server as long as confirm the identity of the domain node, greatly reducing the central node assignments. As for the sender generates a message authentication code and the decryption key for recipient are still the central node to complete, without the help of the domain root. This prevents the domain root to invade privacy of users.
- When they upload the information of themselves is uploaded by layers rather than directly to the central node in order to authenticate users in step by step, and can withstand the distributed denial of service attacks to the root node. When the root node downstream, because the user identity has been verified, it is transmitted directly to user mailbox, in order to avoid the domain root to violate user privacy. The length of message in this program is fixed and resists collusion attack.
- The message of certification sending of sender and certification reading of the recipient are stored in the PKG to prevent any party deny had sent / read the message, which ensures non-repudiation of

messages. PKG can also record the message of saving the state information and make the message become traceability.

4. Conclusion

The currently secure e-mail system has some problems such as high costs, low efficiency, lacking of relevant security technology to ensure effective integration and so on. IBC-New Email integrate IBC and other related technologies, using new security key distribution protocol to achieve message confidentiality, integrity, authentication, non-repudiation and traceability. IBC-New Email is compatible with existing mail protocols, and does not involve the upgrading of the mail server itself, therefore, the upgrading of the existing mail system costs low and it has the some value of application and promotion.

5. References

[1] Stallings W. Cryptography and Network Security [M]. 4th ed. [S.l.]: Prentice Hall, 2006.

[2] Shamir A. Identity-based cryptosystems and signature schemes [C]//BlakleyG T, Chaum D. Advance in Cryptology-Proceedings of CRYPTO’84. New York: Springer-Verl2006:427-444.ag, Lecture Notes in Computer Science, 1985, 196: 48- 53.

[3] Boneh D, Franklin M. Identity Based encryption from the Weilpairing[C]//Killian J.Advances in Cryptology-Proceedings of CRYPTO’01.Berlin, Heidelberg: Springer-Verlag Lecture Notes in Computer Science, 2001:213- 229.

[4] Dodis Y, Yung M. Exposure-resilience for Free: The Hierarchical ID-based Encrytion Case[C]. Proc.of IEEE Security in Storage Workshop, 2002:45-52.

[5] Al-Riyami S, Paterson K. Certificateless publie key cryptography. Advances in Cryptology-Asiacrypt, Springer-Verlag, 2003: 452-472.

[6] Cha J C, Cheon J H. An Identity-based Signature from Gap Diffie-Hellman Groups[C]//Proc.of PKC’03. Miami, FL, USA: Springer-Verlag, 2003:18-30.

[7] Boyen X, Waters B. Compact group signatures without random oracles[C]// EUROCRYPT 2006, LNCS 4004. Berlin: Springer, 2006:427-444.