Fair and Secure Certified Email Protocol

Kyi Kyi Maw, Ei Ei Khin
University of Technology (Yatanarpon Cyber City), Myanmar

Abstract

To provide fairness and confidentiality is more and important in communication system as more and more security related problems have been encountered in today world. In response to this, solutions to these problems have been proposed and some of these guarantee the desired cryptographic strength to some extent. Some of which consider only guaranteeing the fairness between the participants, integrity, non-repudiation properties and the confidentiality of the mail content is not taken into account. The proposed system is aimed to provide a fair and secure certified email protocol which guarantees the fairness, confidentiality, integrity and non-repudiation properties so that the participants can send and receive their mail in secret form and no one else can see the mail content but only intended user can . In this proposed system, the off-line trusted third party (optimistic) will be participated in case of dispute occurs.

1. Introduction

Communicating via e-mail becomes a common and widely used way among people and businesses of today. In traditional mail system, the receiver cannot get the intended mail from the postman without signing his signature and the sender has to register and describe his identity and address on the envelope. So the receiver cannot deny his mail receipt because his signature can prove that he actually received it and also the sender cannot refuse his mail sending. The sending receipt and the delivery receipt are something that the sender can show to prove the message origin and destination. The receiver's signature acts as evidence of receipt and the sender's registration acts as evidence of origin, these two evidences provide non repudiation of origin (NRO) and non repudiation of receipt (NRR) properties, so fairness between the sender and the receiver is available.

In order for e-mail to be used for important communications, some notion of certified delivery must be provided for users. As far as security is concerned, not only confidentiality but also fairness is important requirements, though some other properties are also desirable in practice. Designing certified email protocols is one of the most important problems related to the fair exchange of electronic information and an irrefutable receipt in the sense that either the sender obtains the receipt from the receiver and the receiver gets the mail, or neither party gets the expected item.

A certified email protocol needs to protect the user who is honest, prevent the accessing and modification of the mail content by dishonest person. In case of dispute occurs, trusted third part should resolve effectively without causing any damage to honest participants. Although TTP is involved in every exchange between the sender and receiver and the sender has to send message via TTP, which is called in-line TTP, can guarantee the desired properties of certified email, this can also lead to long delay for the system when multiuser use the system at the same time. So trying to minimize the TTP involvement in certified email has got more attention in literature during the last years. In response to this, Off-line (optimistic) TTP which participates in the system only when disputes occur is used widely. Although this TTP is not involved in every exchange and the sender does not need to send message via TTP, it can effectively resolve the dispute if the protocol is well designed. In this way, using offline TTP can not only provide the required cryptographic properties for certified email protocol but also reduce the delay of the message exchange process. The proposed system is focused to develop the efficient CEM protocol with offline TTP which can guarantee the desired cryptographic strength and protect honest participants of the system.

2. Related Works

Several protocols for certifying electronic delivery have been proposed in the literature. Zhiyuan Liu, Jun Pang, Chenyi Zhang [1] proposed a development of a CEM protocol with transparent TTP. They intend to be impossible to see whether TTP has been participated in the protocol or not by simply observing the evidences. In their system, only sender and TTP can generate the secret key to encrypt and decrypt the message and the receiver can decipher only when the sender send this key.

In this case, TTP can not only resolve the dispute but also know the secret key which offers the confidentiality property to the system. Some common attacks against Certified Email Protocols are discovered and the countermeasures against these attacks are proposed by Min-Hua Shao, Guilin Wang, Jianying Zhou[2]. They show the situations that replay attack can occur and the dishonest participant can get the desired message and evidence by colluding with the third participant. And then they proposed the protocol which is resistant to this attack by using a timestamp metric and encrypting the IDs of the sender and receiver which is included in the part intended to send to the TTP in case of repudiation. Gamal A. Hussein and Fatama Helmy proposed TSRG (two stage random number generator) based certified mail service (TCMS) [3]. In their system, two-stage random number generator [4] plays a vital role which provides a secure and pseudorandom number in order to secure the transaction between the participants. Time-stamping server is also included in their system for temporal authentication and several messages have to exchange for a single mail.

To avoid the problem that the receiver has a chance to decide whether to receive or not a certified email on the basis of the sender's signature, Nicolás González-Deleito proposed the protocol which offers the receiver the ability to reply to a received mail while not knowing who the sender is [5]. This system does not support the evidence of origin for the receiver. Enhancing Certified Email Service for Timeliness and Multicasting [6] is proposed by Jose Antonio Onieva, Jianying Zhou, Javier Lopez. Their system is aimed to reach timeliness and if the request from the receiver is out of time limit, this request is not resolved by TTP. However, in their main protocol, there is no metric for timeliness although the protocol they revised used the time defined by the sender to reach timeliness. This proposed mail protocol is designed to be a fair and secure certified email protocol which guarantees fairness, non-repudiation, confidentiality and resistance to replay attack.

3. Proposed fair and secure certified email protocol

Ordinary mail offers services such as sending and delivery receipts. The sending receipt and the delivery receipt are something that the sender can show to prove the origin and destination of the message. However, the usage of email for official and security oriented events creates some problems because the email service does not have many desirable features. Users should be able to send important information which needs to be read only by intended receiver via email. There are more competitions between business organizations and their message like business plans and strategies need to be sent secretly and no one else but only the intended user should be read it. It is also the same in pressing businesses. The press which can describe the latest and accurate news earlier than any other can reach the top and become popular. So the news from the reporters to the press should be safe from eavesdropping and be sure that the message is from the authentic sender. So their messages should be sent in secure form so that the one who intercept the message cannot read it. For the above cases, the email service should provide security for sensitive and security oriented messages. In order to avoid undesirable problems, repudiations, and dishonest activities among users, email service should be able to guarantee the required cryptographic properties. The proposed system is aimed to provide a fair and secure certified email protocol which can provide efficient cryptographic strength by providing fairness, non-repudiation, message integrity and confidentiality. The processing steps of the system are as follows:

1. A→B: A,B, H(k(M)), H(k), T_s, EOO_M
2. B→A: EOR_{M1} , $k_{TU}(EOR_{M2})$
3. A→B: k_{BU} (k_{AR} (k, k(M)))
4. B→A: EOR_{M2}

EOO_M = k_{AR}[A,B,H(k(M)),H(k),T_s, (k_{TU} (A,B, H(k(M)), H(k), T_s, k(M), k_{BU} (k)))]
EOR_M = $k_{BR}(EOO_M)=EOR_{M1}+EOR_{M2}$
k_{AU} = A's public key
k_{AR} = A's private key
H = hash function
k = symmetric key
T = Trusted Third Party (TTP)
T_s = starting time to send message

EOO can be used to prove that the sender sent the message and the sender can't deny it because EOO is created using sender's private key and no one else has this key. EOR can be used to prove that the receiver received the message as it is produced using receiver's private key and no one else but receiver can use this key. To encrypt and decrypt the message, the secret key is generated only by the sender. Hash function takes the message as input and produces an output referred to as a hash code to be used for data integrity.

Step 1: The sender id, receiver id, encrypted message using symmetric key, hash codes of ciphertext and symmetric key (H(k(M)), H(k)) and evidence of origin (EOO) are sent to the receiver. EOO is generated by signing the combination of A, B, H(k(M)), H(k), (k_{TU} (A,B, H(k(M)), H(k), k_{BU} (k))) with the sender's private key. In which, the part encrypted using TTP's public key is to be used by TTP in case of dispute.

Step 2: The receiver signed the received EOO using his private key and send first half as first part of EOR and the second half encrypted with TTP's public key. Since the second part is encoded with TTP's public key, sender can't see it and use the combination of these parts as complete EOR.

Step 3: A encrypts the symmetric key and ciphertext using B's private key after signing with his private key and send it to B. B can see that this key is from A because it is signed by A's private key and only B can decrypt and use the key as it is encrypted with B's public key and has to decrypt with B's own private key.

Step 4: B verify the correctness of key and message by comparing the hash value of key and ciphertext received in step 1 with the calculated hash value of key and ciphertext. If the two hashes are matched, B sends the second part of evidence of receipt EOR_{M2} to A.

After these 4 steps, A gets the complete EOR to prove that B has received the message and B gets the message and EOO that can be used to prove that A has sent this message if dispute occurs. In this system, the encrypted message and the key to decrypt it is only sent in step 3 after the sender has received the part of evidence of receipt from the receiver in step 2 so that the receiver cannot get even the encrypted message without returning the evidence. This give a more fair way for the sender and can reduce the message sent in step 1. In this system, the first half of evidence of receipt is sent without encrypting and the second half is in encrypted form. In this way, the sender cannot get the evidence of receipt if he does not send the key and encrypted message in step 3. The receiver can also get fairness too.

Recovery protocol

Recovery protocol is run for the following cases:

Case 1

The recovery protocol is run by B if A does not send the key and encrypted message after receiving the evidence of receipt (EOR_{M1}) by sending the request to TTP as follows:

B→TTP: EOO_M, EOR_{M1}, $k_{TU}(EOR_{M2})$

EOO_M= k_{AR}[A, B, H(k(M)), H(k), (k_{TU} (A,B, H(k(M)), H(k), k_{BU} (k)))]

TTP checks whether the message has been aborted or not. If the message has been aborted, it sends abort message to the requester. If message has not been aborted, TTP verified evidences by comparing hash values contained in the received request. If the hash values are matched,

TTP→B : k_{TR} (k(M),k_{BU} (k))
TTP→A: $k_{TR}(EOR_{M2})$

If not, TTP sends back error message.

Case 2

The recovery protocol is also run by A if B does not send EOR_{M2} in step 4 after receiving the key by sending the following request message to TTP.

A→TTP: EOO_M, EOR_{M1}, k_{TU} (EOR_{M2})

TTP checks validity of message as in case 1 and does the same resolution. Then TTP verified evidences by comparing hash values contained in the received request. If the hash values are matched,

TTP→A: $k_{TR}(EOR_{M2})$

If not, TTP sends back error message.

Case 3

If A did not send the hash value of the valid encryption key in step 1 but sending the hash of wrong key, B has no idea that the key is not valid if the decrypted message is reasonable. In this way, A can get the EOR_M from B without giving the valid key. However, when he used this EOR_M for the message he sent, B can know that the message is differed from the one he decrypted and then ask TTP for help by sending the key and EOO_M that A has sent and the decrypted message.

B→TTP : K_{TU}(EOO_M, H(k(M)),H(k))

TTP compares the hash of the key sent by B with the one in the encrypted part of EOO_M. If they match, then TTP compares the hash of encrypt the message sent by B with the one in EOO_M, if they do not match TTP identifies A as dishonest person and A cannot be used EOR_M as proof any more.

Abort protocol

Abort protocol can be run by A if it does not receive EOR_{M1} from B or it does not want B to receive the message any more.

A→TTP : A,B, k(M), H(k(M)), H(k), T_s, EOO_M , abrt

TTP checks the whether the hashes and timestamps (T_s) are matched those in EOO_M. If they are matched, TTP records the message as aborted and send abort message to both sender and receiver. If the sender tried to replay the previous message sent by the sender can protect by comparing T_s as the starting time to send message cannot be identical for different messages from the same sender. And also the replay attack of the receiver can also be detected in this way. The attack from the receiver by colluding with the third participant to get evidence of origin from TTP can be prevented too as TTP can check the consistency of the sender ID and receiver ID of the original message and the IDs in the request. The mail content is only seen by the sender and the receiver even TTP cannot. So the proposed system is able to provide the confidentiality and can be used for sending sensitive and security oriented information among the participants.

4. Conclusion

Certified email is an important service to deliver important data over the Internet with guaranteed receipt for each successful delivery. In this proposed CEM protocol, off-line (optimistic) TTP would be participated to resolve the disputes. Off-line TTP is not invoked in the protocol execution at all, unless one of the two parties misbehaves or the communication channel is out of order. The proposed system can provide important properties of certified email in order to overcome security related problems with the help of off-line trusted third party (TTP). If the timeliness and abuse-freeness properties are able to be added, the system will be a more efficient system.

5. References

[1] Zhiyuan Liu, Jun Pang, Chenyi Zhang, Extending A Key-Chain Based Certified Email Protocol with Transparent TTP

[2] Min-Hua Shao, Guilin Wang, Jianying Zhou, Some Common Attacks against Certified Email Protocols and the Countermeasures.

[3] Gamal A. Hussein, Fatma Helmy, TSRG based Certified Mail Service (TCMS).

[4] Gamal Hussein, Yasser Dakroury, Bahaa Hassen, Ahmed Badr, Two-Stage Random Generator (TSRG); Attack-Oriented Design and Implementation, S ´ Ecurit´e des Communications sur Internet– SECI02, september 2002.

[5] Nicolás González-Deleito , No Author-Based Selective Receipt in Certified Email with Tight Trust Requirements, proceedings of the 4th International Workshop for Applied PKI.

[6] Jose Antonio Onieva, Jianying Zhou, Javier Lopez, Enhancing Certified Email Service for Timeliness and Multicasting.