A Fair Certified Email Protocol with Message Confidentiality

Kyikyi Maw, and Eiei Khin

***Abstract*—**In order to provide secure and fair communication system is more important nowadays. Because more and more security related problems and cyber crimes are the most frequently heard topic all over the world. Therefore, so many certified email protocols have been proposed to cope with these problems. Security of the mail content is not taken into consideration in some of these protocols. So, 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 the mail in fair and secret form and no one else but only the intended user can see the mail content. In order to resolve the disputes and provide fairness, off-line (optimistic) trusted third party will be participated in this system.

***Keywords*—**Confidentiality, Fairness, Integrity, Non-repudiation, Off-line (optimistic) Trusted Third Party.

I. Introduction

NOWADAYS, email has become the most widely used means in daily communication on the internet because it is faster, less expensive and more convenient. The usage of email for official events creates some problems because, in its simplest from, the email service does not have many desirable features. Ordinary mail offers services such as sending and delivery receipts, which can be used to prove the message origin and destination. Certified email tries to deal with these problems using certified email protocols. Certified email protocols have to guarantee that a participant exchanges a message from a receipt, which the receiver should release at the end of the transaction. Indeed, the aim of such protocols is to provide a procedure for the secure exchange messages, which is resistant to possible attempts of cheating by the participants.

Therefore, certified email protocols have to guarantee several standard properties like non-repudiation of origin, non-repudiation of receipt, authenticity, integrity, confidentiality, fairness, timeliness and temporal authentication. Non-repudiation means if an item has been sent from Alice to Bob, Alice cannot deny the origin of the item and Bob cannot deny the receipt of the item. A certified email protocol is said to be fair if it ensures that during the exchange of the items, no party involved in the protocol can gain a significant advantage over the other party, even if the protocol is halted for any reason. In other words, 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 party should resolve effectively without causing any damage to honest participants. The communication channels between the TTP and the other agents are assumed to be resilient, i.e. all data is delivered after a finite, but unknown amount of time. The communication channels between the other agents are assumed to be unreliable, i.e. data may be lost.

Recently, many researchers have been working on finding certified email protocols that satisfy the above properties, and several email protocols with different types of TTP have been proposed. TTP can be in-line TTP, online TTP or off-line (optimistic) TTP. A trusted third party acting as a delivery authority, intervening in each transmission between the sender and the receiver, is called in-line TTP. Although this type of TTP can guarantee the desired properties of certified email, this can also lead to a communication and computation bottleneck. An online TTP does not handle the items to be exchanged, but is necessary in each invocation of the main protocol. M. Abadi, N. Glew, B. Horne, and B. Pinkas [1], R.Deng, L. Gong, A. Lazar, and W. Wang [2] and J. Zhou and D. Gollmann [3] proposed systems with this type of TTP.

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 that participates in the system only when disputes occur is widely used today. 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.

II. Related Works

Several protocols for certifying electronic delivery have been proposed in the literature. Zhiyuan Liu, Jun Pang, Chenyi Zhang [4] proposed a development of a CEM protocol with

Kyikyi Maw is with the Faculty of Information and Communication Technology, University of Technology (Yatanarpon Cyber City), Pyinoolwin, Myanmar (e-mail: kyimaw83@gmail.com).

Eiei Khin is with the Faculty of Information and Communication Technology, University of Technology (Yatanarpon Cyber City), Pyinoolwin, Myanmar (e-mail: ei2khin@gmail.com).

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[5]. 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) [6]. In their system, two-stage random number generator [7] 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 [8]. This system does not support the evidence of origin for the receiver. Enhancing Certified Email Service for Timeliness and Multicasting [9] 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. Two generic, optimistic and efficient schemes for fair certified email deliver are proposed by Guilin Wang, Feng Bao, Kenji Imamoto and Kouichi Sakurai [10]. Their schemes provides fairness and timeliness with the help transparent TTP.

Above works use a new session key for each message exchange to be used in encrypting the message and use the symmetric encryption algorithm. The proposed system uses the public key encryption algorithm and public key of the receiver to encrypt the message in order to provide the message confidentiality. 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.

III. Proposed Fair Certified Email Protocol With Message Confidentiality

Certified email protocols are designed to achieve fair-exchange of a message and a receipt between two potentially mistrusting parties. A protocol is said to be fair, if it is guaranteed that the message receiver can get the email content if and only if the message sender obtains an irrefutable receipt from the receiver. Moreover, users should be able to send important information which needs to be read only by intended receiver via email. In this paper, a CEM protocol with offline (optimistic) trusted third party that can guarantee the fair exchange of message in a secret form between the sender and the receiver is proposed. To provide the secrecy of message, the public key of the receiver is used as message encryption key instead of a new session key. The protocol works with three sub-protocols: exchange sub-protocol, recovery sub-protocol and abort sub-protocol.

A. Exchange sub-protocol

If both participants behave honestly and send the respective items to the other properly, the message exchange procedure follows the exchange sub-protocol. The exchange sub-protocol is as follows:

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

$EOO_M = k_{AR}[A,B,H(k_{BU}(M)),T_s, (k_{TU} (A,B, H(k_{BU}(M)), T_s, k_{BU}(M))]$
$EOR_M = k_{BR}(EOO_M)=EOR_{M1}+EOR_{M2}$

EOO_M = evidence of origin of the message
EOR_M = evidence of receipt of the message
A = sender of the message
B = receiver of the message
k_{AU} = A's public key
k_{AR} = A's private key
$k_{BU}(M)$= the message encrypted with B's public key
H = hash function
T = Trusted Third Party (TTP)
T_s = starting time to send message

EOO_M is generated by the sender by using his private key in order to prove that the sender sent the message. In which, not only the message that the sender wishes to send the receiver but also the part enciphered with TTP's public key intended for TTP to be used in case of disputes. And also EOR_M is generated by the receiver by signing upon the received evidence with his private key to be used as a proof that the receiver is actually received the message. T_s is intended to be used as a nonce for the purpose of protecting the replay attacks. Instead of a random value, the message sending date and time is used as the nonce value and named as T_S.

At first, the sender sends the IDs of the sender and receiver, the hash value of encrypted message, the time stamp value (T_S) and the evidence of origin of the message (EOO_M) to the receiver. After checking the correctness of the evidence, the

receiver generates the evidence of receipt of message (EOR_M). Then, the receiver replies the first half of EOR_M in plaintext form and the second half in encrypted form using TTP's public key so that the sender cannot get the complete evidence of receipt at the second step of the protocol but part of the evidence.

Upon receiving the evidence from the receiver, the sender checks the signature on the first part of evidence which is not encoded. If correct, the sender sends the signed encrypted message $k_{AR}(k_{BU}(M))$ to the receiver in turn as the third step of the protocol. After getting this, the receiver generates a hash value from the received message and verifies the new hash value is in correspondence with the one in the message received at the first step of the protocol. If the message is correct, the receiver replies the plaintext form of the second half of the evidence of receipt of message to the sender. 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.

B. Recovery sub-protocol

The recovery procedure will be launched by one of the participants (the sender or the receiver) once the other participant misbehaves on the message or the communication channel is out of order. If the sender (A) refuses to comply in Step (3) or gives an unreasonable date or location, the receiver (B) is allowed to launch the recovery sub-protocol provided that he has sent EOR_M in step (3), but has not received the encrypted message by sending message of the recovery sub-protocol to TTP as follows:

$$B \rightarrow TTP : A, B, H(k_{BU}(M)), T_s, EOO_M, EOR_{M1}, k_{TU}(EOR_{M2}), rec$$

where rec is used to identify the recovery request.

On receipt of a message of recovery, TTP has to check the correctness of the signatures on the evidences and whether the message has been aborted or not first. If the message has been already aborted, TTP sends error message to B. If all the above checks succeed, TTP retrieves plaintext form of EOR_{M2} from the recovery request message and the encrypted message from the EOO_M. TTP records the message as recovered and signs the retrieved items by using its private key and sends them to the sender and the receiver respectively as follows:

$$TTP \rightarrow B : k_{TR}(k_{BU}(M))$$
$$TTP \rightarrow A : k_{TR}(EOR_{M2})$$

The sender is also allowed to launch the recovery protocol when the receiver fails to send EORM2 after receiving the key by sending the following recovery request message to TTP.

$$A \rightarrow TTP: A, B, H(k_{BU}(M)), T_s, EOO_M, EOR_{M1}, k_{TU}(EOR_{M2})$$

TTP checks if the message has been aborted or not and the correctness of the signatures on the evidences. If the message has been already aborted, TTP sends the error message as before. If both checks succeed, TTP records the message as recovered and does the same resolution as in above case by sending the following items to the sender and the receiver respectively.

$$TTP \rightarrow A : k_{TR}(EOR_{M2})$$
$$TTP \rightarrow B : k_{TR}(k_{BU}(M))$$

This sub-protocol can also be launched by the receiver if the sender does not send the correct message in step 3 of the exchange sub-protocol. If A did not send the hash value of the valid message in step 1 but sending the hash of wrong message, B has no idea that the message is not valid if the decrypted message is reasonable. In this way, A can get the EOR_M from B without giving the valid message. 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 recovery request message including the message and EOO_M that A has sent and EOR_M.

$$B \rightarrow TTP: A, B, H(k_{BU}(M)), T_s, k_{BU}(M), EOO_M, EOR_{M1}, EOR_{M2}, rec$$

Then, TTP compares the hash of the message sent by B with the one in the encrypted part of EOO_M. If they do not match, TTP identifies A as dishonest person, records the message as aborted and A cannot be used EOR_M as evidence any more.

After launching the recovery sub-protocol by either the sender or the receiver, both of them gets their desired items respectively.

C. Abort sub-protocol

The abort sub-protocol will also be launched by one of the participants (the sender or the receiver) once one of participants is unwilling to continue the exchange protocol any more. If A wants to abort the message exchange after sending the message in step (1) or not receiving EORM from B in second step of exchange protocol, then A sends abort request message to TTP as follows:

$$A \rightarrow TTP : A,B, H(k_{BU}(M)), T_s, EOO_M , abrt$$

where abrt is used to identify the abort request.

TTP verifies the signature, hash value and T_s on EOO_M and checks if this message is already aborted or recovered. If it is already recovered, it sends recover message to both participants and if it is already aborted, it sends abort message. If all the above checks succeed, then TTP records the message as aborted and sends abort message to both participants. If the receiver wishes to launch the abort protocol, TTP will deal with the request in the same way as the above case.

IV. Security Analysis Of The Proposed Protocol

In case of a dispute, EOR_M alone from the sender is sufficient to prove that the receiver has received the message. As to the authenticity of the message, the receiver is able to

prove every third party that the message is actually from the sender by verifying the sender's signature on EOO_M after extracting the message from the ciphertext. Since presenting (M, EOO_M) is sufficient for the receiver to prove that M is originally from the sender, the protocol satisfies strong fairness and non repudiation of origin and receipt.

In any exchange of message between the two participants, the sender can always launch the abort sub-protocol after she sends out the first message, so that TTP will send back either an abort message or EOR_M depending on whether a recovery message has already arrived at TTP or not. The receiver can launch the resolve sub-protocol any time after receiving the first message and will get either an abort token or the ciphertext depending on the communication between the sender and TTP. The resilient channels between TTP, the sender and the receiver guarantees that the above procedures terminate in a timely manner.

If both the sender and receiver behaves honestly to follow the protocol and no network error occurs which means there is no large network delay, only the exchange sub-protocol is run and will terminate at a state where the sender gets the desired evidence of receipt and the receiver gets both the message and the evidence of origin.

As the message intended for the receiver is encrypted with his public key, only the receiver can see the message. No one else even TTP cannot see the message content as the message contained in EOO_M is encrypted with the receiver's public key although this part is aimed to be used by TTP to resolve the disputes. So the proposed system guarantees the message confidentiality between the sender and receiver. Moreover, there is no need to generate a new session key for each message exchange in this system as the public key of the receiver is used instead.

V. 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. The proposed system can provide important properties of certified email in order to cope with security related problems with the help of off-line trusted third party (TTP). If the abuse-freeness property is able to be added to this protocol, the system will be more efficient.

References

[1] M. Abadi, N. Glew, B. Horne, and B. Pinkas, "Certified email with a light on-line trusted third party: Design and implementation", in *Proc. of 2002 International World Wide Web Conference (WWW'02)*, pp. 387-395. ACM press, 2002.

[2] R. Deng, L. Gong, A. Lazar, and W. Wang, "Practical protocol for certified electronic mail", *Network and Systems Management Journal*, 1996, 4(3): 279-297. http://dx.doi.org/10.1007/BF02139147

[3] J. Zhou and D. Gollmann, "Certified electronic mail", in *Computer Security - ESORICS'96*, LNCS 1146, pp. 160-171. Springer-Verlag, 1996. http://dx.doi.org/10.1007/3-540-61770-1_35

[4] Z. Liu, J. Pang, C. Zhang, Extending A Key-Chain Based Certified Email Protocol with Transparent TTP.

[5] M. H. Shao, G. Wang, J. Zhou, Some Common Attacks against Certified Email Protocols and the Countermeasures.

[6] G. A. Hussein, F. Helmy, TSRG based Certified Mail Service (TCMS).

[7] G. Hussein, Y. Dakroury, B. Hassen, A. Badr, Two-Stage Random Generator (TSRG); Attack-Oriented Design and Implementation, S ´ Ecurit´edes Communications sur Internet– SECI02, September 2002..

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

[9] J. A. Onieva, J. Zhou, J. Lopez, Enhancing Certified Email Service for Timeliness and Multicasting.

[10] G. Wang, F. Bao, K. Imamoto, K. Sakurai, Generic, Optimistic, and Efficient Schemes for Fair Certified Email Delivery

Kyi Kyi Maw received Bechelor of Computer Technology from University of Computer Studies; Yangon in Myanmar. She completed the master course from University of Computer Studies since 2009 and especially studied and finished the thesis by Digital Image Processing. She is working now in University of Technology (Yatanarpon Cyber City) as a tutor under the Faculty of Information and Communication Technology. Now, she is a Ph.D student in this University which is near Pyin Oo Lwin, Upper Myanmar and mainly studying about Cryptography and Network Security. Her fields of interest are Digital Image Processing, Cryptography and Networking.