AN IMPROVED CERTIFIED E MAIL PROTOCOL BASED ON AUTHOR BASED SELECTIVE RECEIPT

Ranadeep Mukherjee, Ambar Dutta[1]
[1]Department of Computer Science and Engineering, Birla Institute of Technology
Ranadeep.m@bitmesra.ac.in, adutta@bitmesra.ac.in

ABSTRACT

The paper proposes improvements to the Certified E mail Protocol proposed by Imamoto and Sakurai in terms of implementing the 'No Author Selective receipt' concept. It also aims to provide complete anonymity for the communicating parties as well as protecting the sender from being adversely effected by the collusion between the Receiver and the Notice Board.

KEYWORDS

Certified E mail, Notice Board, Selective Receipt

1. INTRODUCTION

Nowadays, e-mail has become one of the most widely used communication medium. Because of its low cost characteristics and rapid delivery of messages, e-mail is increasingly used in place of ordinary mail. However, the e-mail service exposes users to several risks related to the lack of security during the message exchange. Furthermore, regular mail offers services which are usually not provided by e-mail, and which are of crucial importance for "official" events. Certified e-mail tries to provide users with additional guarantees on the content and the delivery of the messages, making e-mail equivalent and in some cases more convenient than the ordinary paper-based mail service. These protocols provide the following property: user Bob receives an e-mail message from user Alice if and only if the latter receives a receipt for this communication, i.e., a proof that the message has been delivered to the recipient. The receipt is such that the recipient cannot deny having received the message. This feature is called non repudiation. In order to implement non repudiation many of the protocols use a Trusted Third Party (TTP) [1] whose job is to ensure that any disputes which may arise between the communicating parties can be settled in a fair, unbiased manner. TTPs can be of various kinds including inline, offline etc. Certified e-mail protocols provide other features like confidentiality of the message, proof of integrity, and so forth.

A few of the features have been described [2]

- **Fairness:** Both users can obtain the result each one desires or neither of them does.
- **Authentication:** Both users can confirm that his partner is certainly the target partner.
- **Confidentiality:** Adversary cannot decrypt a message of Certified E-mail.
- **Integrity:** In the middle of a protocol, adversary and partner cannot rewrite a message.
- **Anonymity:** Adversary cannot guess who are communicating.

DOI:10.5121/ijcis.2012.2407

The basic system that has been described in this paper consists of three parties namely an entity who transmits a Certified E-mail (called *Sender*), an entity who receives it (called *Receiver*), and an entity who mediates this system (called the notice board). All entities know the used encryption technologies (that is, a symmetric key encryption, a public key encryption, a hash function, digital signature method). In this system the knowledge of someone's identity is the same as the knowledge of his public encryption key and verification key. While several papers deal with the features of fairness, confidentiality and non repudiation, very few papers deal with the concept of anonymity. Also most protocols do not implement "no author selective receipt" where the receiver does not get any information regarding the sender's identity unless it agrees to receive the message the sender wants to send. For sensitive communication often it is necessary to keep the identity of the communicating parties hidden from the outside world. Our paper is going to try and discuss this feature. We initially describe an existing protocol that implements anonymity partially and later try to improve it by proposing a simple way to implement it fully.

The rest of the paper has been organized as follows. In Section 2 the previous work on Certified E mail Protocols have been discussed. Section 3 describes the existing protocol proposed by Imamoto et al in brief. Section 4 states the limitation in the existing protocol and suggests an improved protocol to overcome those limitations. Section 5 contains the detailed analysis of the enhanced protocol. Finally the activity taken up in this paper is summarized in Section 6.

2. RELATED WORK

In the literature we have found a large number of protocols proposed by several researchers for certified e-mail using a third party during the exchange of the message. Bahreman and Tygar [3] proposed an inline protocol requiring six messages to be sent among the parties. In their protocol the sender sends the e-mail message to the TTP, which returns a proof of mailing. Then, the TTP encrypts the message with a session key and sends it to the recipient, who signs the cipher text and returns the signature to the TTP. Finally, the TTP sends the receipt to the sender and the session key to the recipient. Deng et al. [4] proposed two inline protocols requiring four messages to be sent among the parties. In particular, the second protocol preserves the confidentiality from the TTP, while the first one does not. Coffey and Saidha [5] proposed a non-repudiation protocol which relies on an external time-stamping authority to state the non-repudiation of origin and destination evidence time. Several non-repudiation protocols which have been applied to certified e-mail have been proposed by Zhou and Gollmann. In [6] the authors present a protocol that requires five messages. The key idea is that the sender and the receiver exchange the signatures on the encrypted message and then interact with the TTP to recover the key and the non repudiation-proofs. In [7] another protocol is proposed where the e-mail message is transmitted from the sender to the receiver through a sequence of trusted third parties. The role of these parties is to deliver the message, collect the receipt signed from the receiver, and route them back to the sender. Schneier and Riordan [8] proposed a protocol in which the sender encrypts the e-mail message with a session key and sends it to the receiver. Then, the receiver asks the sender to publish the session key on a secure database server at a certain time. This message is signed by the receiver and sent to the sender. Afterwards, the sender submits the session key to the server; then, the receiver gets it and decrypts the e-mail. Abadi, Glew, and Pinkas [1] proposed an inline protocol requiring four messages. The protocol does not require any public-key infrastructure. However, the protocol assumes that the TTP has some public keys and that some other authentication mechanism is provided (such as a shared secret) among the participants. Franklin and Reiter [9] introduce the notion of a semi-trusted third party for the fair exchange problem. Their protocol is online as it requires the TTP to be involved in any transaction. The TTP can sometimes fail or misbehave but it cannot conspire with either of the parties involved in the exchange. Their model is actually more restrictive, it is assumed that at most one party misbehaves. If the sender cheats, for instance, then the recipient and the trusted third party must

be both honest. This also implies that if the TTP misbehaves then, by definition, the other two parties are honest and, in principle, they could simply exchange their items by themselves.Certified E-mail system needs some requirements other than fairness, such as authentication, confidentiality, integrity, non-repudiation, and efficiency. Moreover, there is a manner called send-and-forget. This manner is as follows: after sending a message, a sender does not have the necessity of waiting for a receiver's reply, and the receiver can obtain a desired item without a sender's help.

3. EXISTING PROTOCOL PROPOSED BY IMAMOTO AND SAKURAI

The protocol proposed by Imamoto and Sakurai [2] was an extension of the protocol proposed by Scheiner and Riordon [8]. One of the main drawbacks in the earlier protocol [8] was the fact that confidentiality of the message was compromised. This was because the symmetric key with which the message was initially encrypted is sent by the sender to the receiver across the same unsecured network at the end of the protocol. Any malicious third party can simply get hold of the encrypted message and wait for the key to be sent by the sender. Once the sender sends the key across the network, it can capture the key and encrypt the message.

Imamoto and Sakurai solved this problem by encrypting the message with the public of the receiver i.e. E_B (E_k (M)) where E_B is the receivers public key and E_k () is the symmetric key encryption using the key K .Hence although any third party could capture the symmetric session key, he was unable to use it to decrypt the message because the message itself was encrypted by the public key of the receiver. The protocol has been explained with the help of the following figure.

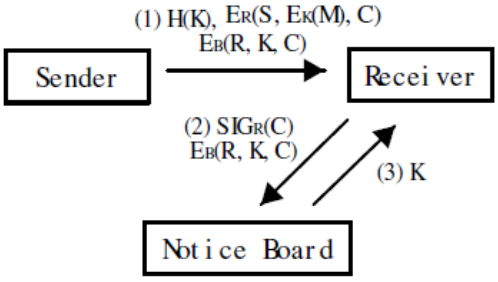

Figure 1: Protocol Proposed by Imamoto et.al

In this protocol initially the sender sends the message M encrypted with the session key K which is in turn encrypted by the public key of the receiver. The key K itself is encrypted by the public key of the Notice board (which acts as the trusted third party). After the receiver receives the message from the sender it verifies the sender's signature and once that has been done successfully ,it forwards the encrypted key to the notice board with it's signature. The notice board on successful verification of the receiver's signature will decrypt the message received using its private key and get the symmetric key K. The notice board will sent the key to the receiver and publish the message it received from the receiver (message 2) in its public directory. The sender can obtain that message from their and it becomes the proof of receipt for the sender. The protocol consists of three steps and three rounds of encryption. 'C' consists of the sender's digital signature. It should be noted that the message C=<dig_s(H(K),Ek(M))>.

4. PROTOCOL ENHANCEMENT

The protocol has three basic limitations. It can only provide partial anonymity. Anonymity means that a third party is unable to find out the identities of the communicating parties. In this protocol the identity of the sender is hidden as it is encrypted with the public key of the receiver in Step 1 of the protocol. So it is hidden from every other party including the notice board. But as we can clearly see in step 2 the receivers identity is encrypted using the public key of the notice board and hence the identity of the receiver would be visible at least to the notice board. Hence this protocol is unable to provide complete anonymity. Although the authors have assumed that the leakage of the receiver's identity might not be a very serious issue there might be cases where both identities must be hidden from all other parties including the Notice board because there is always a possibility that the notice board might get corrupted and act in a dishonest manner.
Another problem with the existing protocol is the fact that the fairness can be broken because of a conspiracy between the Notice board and the Receiver. There may be a case that after the notice board publishes the secret key in its public directory it colludes with the receiver and removes the proof of receipt before the sender actually gets it. It is very difficult for the sender to understand the attack because he is not able to infer whether the receiver has not yet received the key or there is a conspiracy between the notice board and the receiver. A third limitation arises as the protocol does not implement "no author selective receipt". In message 1 'C' contains the digital signature of the sender. So after the receiver obtains message 1 it can refuse to receive the message. But he still obtains the sender's identity by using 'C'.

The authors propose a potential solution for both the problems as follows:

In order to implement "no author selective receipt" the sender removes 'C' from the portion $E_R(S,C, E_k (M))$ of message 1.In the first step when the receiver gets message1 it cannot get any idea of the identity of the sender .Only after the receiver sends message2, it is allowed to see and verify the sender's identity. The detailed explanation for the same has been provided in the section below.

Anonymity in this protocol can be implemented fully if the receiver's identity is kept hidden from the notice board. A part of the message in step 1 of the existing protocol is $E_B(R,K,C)$ where R is the receiver's identity, K is the symmetric encryption key. Now we change that portion of the message to $E_B(K,C)$.This means only the symmetric encryption key K is being encrypted with the public key of the notice board E_B. Another problem comes up as the sender can be deprived of the receipt due to the collusion of the Notice board and the receiver. In step 2 of the existing protocol it can be seen that the receiver sends the following message to the notice board

$$Sig_R(C),E_B(R,K,C)$$

So the notice board gets hold of the receipt meant for the sender. So if the Notice board becomes dishonest it may refuse to provide the receipt to the sender. As a solution the authors propose that Step 2 should send two messages to two different parties. While $Sig_R(H(K))$ is sent to the sender $<Sig_R(H(K),E_B(K,C)>$(as in message m3 of step2 of the protocol described below) is sent to the Public Notice board. The effect of the changes will be discussed in the Analysis section later on. So the modified protocol will consist of the following set of steps:

Step 1

The sender will create message m1=<$H(K),E_R(S, E_k(M)),E_B(K,C)$> where H(K) is a collision resistant hash function of the session key K and the message M is encrypted through the key K.E_R and E_B refers to the public key of the Receiver. After creating the message he sends the same to the receiver.

Step 2

After he receives the message the receiver will decrypt $E_R(S,E_k (M))$. Next it will create two messages: m2=<$Sig_R(H(K))$> and m3=< $Sig_R(H(K),E_B(K,C))$>.It sends m2 to the sender and m3 to public notice board.

Step 3

The notice board receives m3 and verifies the signature of the receiver. If the signature is verified then the notice board decrypts $E_B(K,C)$ to obtain the session key K and sends it to the receiver R in form of m4 =<$K,E_R(C)$> . 'C' is encrypted so that the confidentiality feature of the protocol can be maintained. The receiver receives key K and it can verify the identity of the sender of m1 from 'C'. Finally the receiver will use K to decrypt the message $E_K(M)$.

5. ANALYSIS AND RESULTS

This section analyses the proposed protocol to see how efficiently it can counter the problems described earlier. In the modified protocol the identities of both the sender and the receiver remains hidden from all outsiders. The identity of the sender S is encrypted by the public key of the receiver in Step 1 of the protocol hence only the receiver R can view the sender' identity. On the other hand unlike the protocol proposed by Imamoto et.al in this protocol the receiver's identity is not compromised to the Notice board because in message m1 the only data that is encrypted by the public key of the notice board is the session's key K and 'C'. Hence in this protocol anonymity can be implemented fully i.e. both for the sender and the receiver.

In the previous protocol the receiver could collude with the notice board and stop the sender from receiving the receipt from the receiver. In this protocol this problem has been countered in step 2 where instead of sending the entire message to the notice board the receiver needs to send message m2 to the sender and message m3 to the Notice Board. Hence the sender receives the copy of the receipt without depending on the notice board even when the notice board colludes with the receiver. However after getting the receipt the sender cannot stop the receiver from receiving the decryption key as the Notice Board holds $E_B(K,C)$ and it can send the same to the receiver. Hence fairness is maintained in this protocol. The concept of No author Selective Receipt is also implemented in the modified protocol as the receiver is unable to know the identity of the sender of the message M until the receiver accepts to receive the message by sending the NRR (Non Repudiation of Receipt) message to the former. When the receiver receives m1 in step 1 of the protocol it cannot gain any knowledge about the identity of the sender from it. Only after it sends the message m2 to the sender confirming its readiness to receive the message M, it can verify the identity of the sender by checking the message m4 which it receives from the notice board. It should be noted that the receiver has the right to refuse to receive the message M by not replying to m1 send in step 1 of the protocol.

The protocol also implements confidentiality as the message M is encrypted by the public key of the receiver so no third party is able to tamper with the message privacy. The sender of every message is confirmed by verifying their digital signatures, hence providing authentication and

also non-repudiation. But this protocol requires one extra round as compared to the previous protocol as in this we are sending four messages while in the previous protocol we were only sending three. In most certified E mail systems it is assumed that a message is never lost in transmission because if that happens and the concerned party cannot detect it fairness is broken. But this assumption is difficult to implement for most unstable communication channels. But using a Public Notice board it can be realized for such because even if a message is lost, the same can be accessed from the public notice board by either party. Hence this system with a notice board is considered suitable for an unstable medium.

The table below shows the comparison between the protocol proposed by Imamoto et.al and the one proposed by the authors in this paper.

	Imamoto et.al[2]	**Proposed Protocol**
Anonymity	YES[Partial]	YES[Complete]
Sender dependent on Notice Board for receipt	YES	NO
Rounds	3	4
Confidentiality	YES	YES
Fairness	YES	YES
No Author Selective Receipt	NO	YES

Table 1: Comparison between the existing protocol and the proposed protocol

6. CONCLUSION

In this paper, we have presented a protocol for certified email delivery by extending the known protocol proposed by Imamoto et. al. The protocol proposed by Imamoto authenticates the messages by checking the digital signatures associated with each message and implements confidentiality by encrypting the encrypted message with the public key of the receiver. It is also able to protect the sender's identity from every other party but unfortunately the receiver's identity is exposed to the Notice Board. The protocol proposed here aims at providing receiver's anonymity as well with a simple enhancement that has already been described. In the proposed protocol, the receiver is not dependent on the notice board for receiving the proof of receipt for the message from the receiver. Moreover the receiver is not allowed to get any information regarding the identity of the sender of the message until it confirms its willingness to receive the message in question. Future work in this regard would look at ways for implementing the system under various environments.

REFERENCES

[1] M. Abadi N. Glew, B. Horne and B. Pinkas "Certified Email with Light On-line Trusted Third Party: Design and Implementation", Proceedings of Eleventh International World Wide Web Conference, ACM Press, New York,2002, pp 91-97.

[2] Kenji Imamoto, Kouichi Sakurai, v"Certified E-mail Systems Using Public Notice Board" 14th International Workshop on Database and Expert Systems Applications, 2005 pp.460-465.

[3] Bahreman and J. D. Tygar "Certified electronic mail". Proceedings of the Symposium on Network and Distributed Systems Security, 1994 , pp 3-19.

[4] R. H. Deng L. Gong, A. A. Lazar, and W. Wang "Practical protocols for certified electronic mail". Journal of Network and System Management, vol. 4, issue 3, 1996, pp 279-297 .

[5] T. Coffey and P. Saidha "Non-repudiation with mandatory proof receipt". ACM SIGCOMM Computer Communication Review volume 26 Issue 1,1996, pp 6 – 17.

[6] J. Zhou and D. Gollmann "An efficient non-repudiation protocol". Proceedings of The 10th Computer Security Foundations Workshop. IEEE Computer Society Press,1997, pp 126-132.

[7] J. Zhou and D. Gollmann "Certified electronic mail". Proceedings of ESORICS '96, volume 1146 of Lecture Notes in Computer Science,1996, pp 160-171.

[8] J. Riordan and B. Schneier "A certified E-mail protocol with no trusted third party". Proceedings of the 13th Annual Computer Security Applications Conference, 1998, pp 347-352.

[9] M. Franklin and M. Reiter. "Fair exchange with a semitrusted third party" Proceedings of ACM Conference on Computer and Communications Security, 1997.