THE JOURNAL OF CHINA UNIVERSITIES OF POSTS AND TELECOMMUNICATIONS
Volume 14, Supplement, October 2007

WEN Dan-yan, TONG Cheng-gang, XIA Guo-ping

An email system with non-repudiation service

CLC number TN915 Document A Article ID 1005-8885(2007) S1-0124-07

Abstract Based on a non-repudiation protocol NRPUM, which provides point-to-point non-repudiation services, this paper proposes a non-repudiation solution to secure email systems. Specifically, non-repudiation evidence is used at every hop between relay nodes so that an evidence chain is formed between end hosts. An email non-repudiation delivery system is then developed based on this concept. Our experiment results show that the solution is feasible and the system is effective.

Keywords electronic mail, non-repudiation protocol, SMTP, POP3

1 Introduction

Email is becoming an integrated routine of peoples' daily life, therefore, all email principals should take corresponding social responsibilities. The basic email protocols that we use widely today cannot collect Email's evidence of delivery (EOD), nor can they assert each principal's duty. If an email delivery system could provide email proofs such as evidence of original (EOO), EOD and evidence of recipient (EOR), everybody would be forced to take his legal duty when he uses email. As a result, many email delivery security issues we have today such as spam, email spoofing and email delivery repudiation would be reduced or even eliminated.

Most related research work, such as META signatures [1], PGP [2], S/MIME [3] mainly focus on non-repudiation among mail transport agents (MTA). Others, such as certified mail mechanisms, focus on non-repudiation among user agents (UA).

There are many certified mail protocols in the literature [4–6]. Most of them rely on a certain trusted third party (TTP) that serves as a mediator. The disadvantage of these protocols includes heavy message overhead and low efficiency, as more interaction is needed. Micali proposed a simple and fast protocol [7] for fair electronic exchange using an off-line TTP, and therefore improved transaction efficiency to some extent. But Micali's proposal incurred unfairness among principals. Ferrer-Gomila et al. proposed a FPH certified mail protocol [8] that employs a three step session to provide fairness while maintains efficiency.

In this paper we investigate the use of certified mail mechanisms and non-repudiation protocols to achieve non-repudiation between a UA and a MTA. Specifically, our work is based on a non-repudiation protocol called NRPUM protocol [9], which was proposed by Xia and Liu in 2007. Compared to other related protocols, NRPUM has the following merits:

1) It provides non-repudiation between UA and MTA.
2) It achieves fairness among all principals.
3) It maintains efficiency by using an off-line TTP.

In the following, we present the design and implementation of an Email delivery system with non-repudiation services using the NRPUM protocol.

2 Design goals for email delivery system

Design goals for our email delivery system are as follows:

1) Non-repudiation: A sender can not deny its operation of sending a mail, and a receiver can not deny its operation of receiving a mail.

2) Fairness: Either both principals receive their corresponding evidences, or neither of them does.

3) Resistance: The email delivery system can resist multiple attacks including tamper attack and replay attack.

4) Compatibility: The email delivery system needs to be compatible with protocols such as SMTP [10], POP3 [11] and RFC 2822 etc.

3 Key points analysis

3.1 Classification of non-repudiation services

There are two kinds of ways to implement non-repudiation services: end-to-end implementation and point-to-point implementation.

With end-to-end implementation, the MTA's does not provide non-repudiation when forwarding mail messages. The initiative is in the hands of the email sender. An MTA will forward mail messages even if the mail sender doesn't provide the mail's EOO. As a result, receiver may passively receive a mail message that does not have an EOO. In this case, the implementation for Email non-repudiation totally rely on the will of mail's sender, and email delivery system cannot protect the benefit of the

Received data: 2007-07-01
WEN Dan-yan (✉)
Natural Science Academic Publishing Center of Higher Education Press, Beijing 100029, China
School of Economics and Management, Beihang University, Beijing 100083, China
E-mail: wendy@hep.com.cn

mail's receiver.

With point-to-point implementation, non-repudiation evidences are provided hop-by-hop along the mail's delivery path. The sender needs to exchange information with local MTA and to generate mail's EOO. MTA won't delivery a mail without EOO. In the same way, if the receiver doesn't provide the mail's EOR, its local MTA will refuse to deliver mail messages to him. Even if there is a collusion between the receiver and its local MTA, because the MTAs in previous hops keep the non-repudiation proofs for mail delivery, the receiver couldn't deny the behavior of the mail receiving.

In summary, we choose point-to-point implementation of non-repudiation in our email delivery system.

3.2 The non-repudiation protocol

NRPUM protocol [9], which is designed to provide non-repudiation service between UA and MTA using an Off-line TTP, is more efficient than other similar protocols such as the FPH protocol, as demonstrated by the experiments in recent study [9].

Moreover, the subject of the NRPUM protocol could be any entity in an Email delivery system. Therefore, not only can we use NRPUM protocol between UA and MTA, but also we can use this protocol between MTA and MTA.

3.3 Evidence chain

With point-to-point non-repudiation, all MTAs and UAs along a mail transfer path hold evidences of the mail delivery. The evidence chain which is constructed by these evidences will provide non-repudiation service not only between sender and receiver but also between message relaying nodes.

Because non-repudiation evidences for a specific email delivery are generated by non-repudiation protocol and stored in every node respectively, the relationship among these evidences can be divided into two categories: those belong to the same mail message delivery procedure and those belong to the same specific non-repudiation interaction.

If we include the IP address and ID of next hop node into the hop-by-hop evidence, then starting from evidence at any node we can use the information to locate the next hop node. Consequently, the next evidence can be retrieved based on the corresponding session ID or the unique random value of the session key. Therefore, we can recursively retrieve the entire chain of evidences for a specific mail delivery procedure.

Each UA only holds one piece of proof for each mail delivery procedure because an UA may take a role of either a sender or a receiver. In contrast, MTA may hold two pieces of proofs for a mail delivery procedure because MTA take roles of both sender and receiver and each role will produce the corresponding evidence. If we associate the storage of these two pieces of evidences in the mail delivery label, then from one piece of evidence we can easily find the other piece. So, we can construct evidence chain of a mail delivery, and accomplish non-repudiation service for email system.

Simple mail information (SMI), an internal data structure which is designed to record labels of a specific email delivery, is a key factor for forming evidence chain. The SMI data structure is shown in Fig. 1.

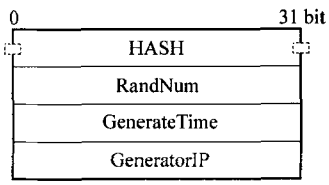

Fig. 1 SMI data structure

SMI consists of four components including HASH, GeneratorIP, Generate time and Rand num.

The 20 byte long HASH field, produced using the SHA1 algorithm, is a digest of a partial header and the full body of the corresponding mail. Specifically, the partial header includes the mail's "From:" field, "To:" field, and "Subject" field. Because all these fields and the mail body remain unchanged during a mail delivery procedure, the HASH field of the SMI is also invariant and is therefore eligible to be chosen as an ID of a specific mail delivery procedure.

Generator IP is the IP address of the node where the SMI is generated and Generate time is the time when the SMI is generated. Rand num is a big random value. Notice that a specific mail may be retransmitted many times. In this case, the HASH and Generator IP fields remain the same. Moreover, even when multiple SMIs are generated at different time, they may have the same Generate time value due to clock granularity, time difference or clock synchronization. Therefore, we need to have a Rand num field to distinguish a variety of mail delivery procedures in case of all Generator IP, Generate time and HASH are the same.

SMI is produced by the first node that provides non-repudiation service in a mail delivery path, and is passed along and reused by all following nodes that are located in the mail delivery path. All nodes store SMI with evidence, so we can retrieve the entire chain of evidence of a specific mail delivery using SMI as index.

We now present the solution for an email delivery system with non-repudiation service as follows.

All nodes which are located in an email delivery path will be deployed with a non-repudiation service module. Each node stores the next hop node's non-repudiation proofs. The email delivery system produces one unique SMI for each email

delivery procedure and store the SMI and proofs in the corresponding node's library. For each email delivery, an evidence chain can be retrieved through the aforementioned recursive hop-by-hop procedure. Therefore, the email delivery system can provide non-repudiation service.

3.4 Compatibility with Standard Email Transport Protocols

Deploying non-repudiation service module at every node may not always be feasible for various network environments. In reality, there may be a number of legacy MTAs and UAs without non-repudiation modules being installed. Being compatible with standard email transport protocols is a key deployment issue for our proposed Email delivery system.

To address this issue, we define two modes of mail delivery: normal delivery mode and abnormal delivery mode.

3.4.1 Normal delivery mode

Normal delivery mode is used to achieve non-repudiation between parties that are deployed with non-repudiation modules. In this case, the exchange message procedure of SMTP and POP3 are shown in Figs. 2 and 3 respectively.

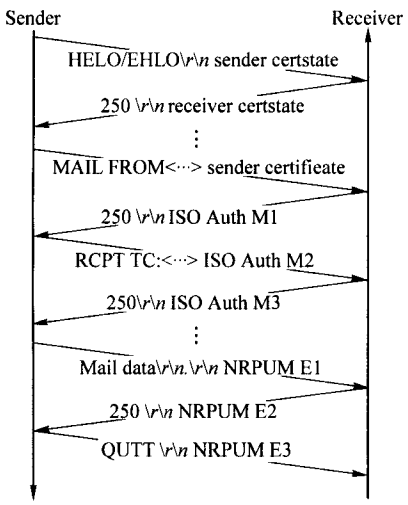

Fig. 2 The message exchange procedure of SMTP with non-repudiation service

The message exchange procedure can be divided into three stages. The first stage is called certificate exchange stage. In this stage, interactive parties exchange and verify theirs certificates. The second stage is called the authentication stage, during which interactive parties authenticate each other's identities. In the third stage, interactive parties carry out NRPUM protocol and produce non-repudiation proofs.

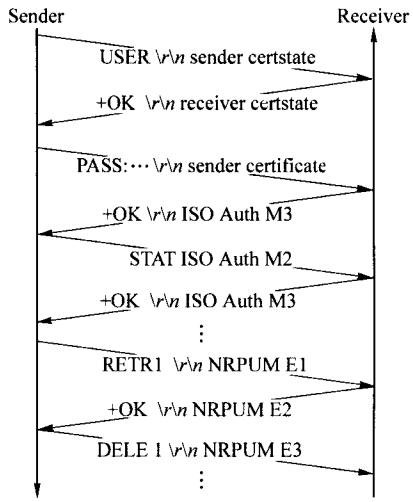

Fig. 3 The message exchange procedure of POP3 with non-repudiation service

POP3 protocol supports delivering multiple Emails in one interactive session. In our scheme, we repeat message exchange procedure of "RETR 1" command, +OK acknowledge and "DELE 1" command to provide non-repudiation service for each Email.

3.4.2 Abnormal delivery mode

The abnormal delivery mode is used to accomplish non-repudiation service in the environment where one of the two parties isn't deployed with non-repudiation service module. In this mode, an email is delivered in common mode. The party which is deployed with non-repudiation service module will keep the delivery proofs of the email that was delivered in common mode. These proofs show that the corresponding email was delivered in common mode.

With abnormal delivery mode, the party that was deployed with non-repudiation service module may intentionally not provide non-repudiation proofs. To prevent this behavior, we design a TTP called time server (TS) that grants this party the permission of abnormal delivery and keeps the proofs of abnormal delivery. These proofs and SMIs at the TS can be used to connect evidence chain links together.

The procedure of abnormal delivery is as follows.

1) Discovering abnormal delivery status. Similar to normal delivery mode, the abnormal delivery mode starts from certificate exchange stage. The node deployed with non-repudiation service module will look for some specific parameters that we defined in our system in email delivery commands and response messages from its corresponding interactive party. If the node finds out these specific parameters, then email delivery system will transfer email message in normal delivery mode, otherwise email delivery system will

transfer email message in abnormal delivery mode.

2) Connecting to TS. Before carrying out following operations, the node deployed with non-repudiation service module need to connect to TS and TS will authenticate its identity.

3) The permission of abnormal delivery. After being authenticated by the TS, the node sends the TS a request for using abnormal delivery mode. The TS will inquire the corresponding interactive party as soon as it receives the request. If the TS fails to connect to the interactive party or if the TS establishes a connection to this interactive party and TS can't receive the corresponding response message or receive the corresponding response message that the TS cannot understand, the TS will assert that the corresponding interactive party is a node without a non-repudiation service module. In this case, the TS sends the node a permission for starting abnormal delivery mode and the TS keeps this permission in its own database. When the node with non-repudiation service module sends a mail, it attaches this permission to the end of mail message to demonstrate to the recipient that this email delivery is in abnormal delivery mode. If the TS receives the corresponding response that it can understand, then the TS deduces that the corresponding interactive node is a node with non-repudiation service. In this case, the TS will reject the request for using abnormal delivery mode, so the sender must send email in normal delivery mode.

4) Email delivery statement. After sending out a mail in abnormal transport mode, the sender needs to send the TS an email delivery request including the email delivery finished message or the reason for fail to delivery email. If the email is delivered successfully, then the TS generates a corresponding email delivery statement and sends it to the sender and keep a record in a local database. If the mail delivery is failed, TS just records the reason of failure. Using email delivery statement, we can confirm the mail transfer time to prevent the sender that receives permission from not sending mail and pretending finished email delivery latter.

In our system, beside signing and issuing email delivery timestamp, the TS also produces, transports and stores permission or refusal of email abnormal delivery and email delivery statement. In order to confirm mail sending time and mail delivery time, the TS inserts the timestamp in permission or refusal of email abnormal delivery and inserts the timestamp in email delivery statement.

The permission produced by the TS includes timestamp and SMI. It is stored at both the TS and each node that participates in the delivery of the email. With abnormal delivery mode, when we collect all proofs of a specific mail delivery in case of raising a mail delivery dispute, the evidence chain may be broken because the node without non-repudiation service module cannot provide proofs of the mail delivery. In this case, we can connect the evidence chain fragments together with the information stored at the TS by the following procedure.

1) After the mail system finishes a mail delivery procedure in abnormal delivery mode, TS and all nodes that participate in this mail delivery procedure will keep their mail's abnormal delivery permission. In a mail delivery procedure, only one permission is attached to the end of mail body. If a mail experiences multiple times of abnormal delivery, then we use the permission that the latter nodes holds to overwrite the permission that the former nodes holds. There are two kinds of permissions and the formats are as follows.

Format 1:

$$\{\text{flag}_{\text{PM}}, R_A, A, C, \text{SMI}, T, \text{S}_{\text{TS}}\{\text{flag}_{\text{PM}}, R_A, A, C, \text{SMI}, T\}\}_{\text{K}_A}$$

Format 2:

$$\{\text{flag}_{\text{PM}}, R_A, A, C, T, S_{\text{TS}}\{\text{flag}_{\text{PM}}, R_A, A, C, T\}\}_{\text{K}_A}$$

Format 1 is used for abnormal sending and format 2 is used for abnormal receiving.

R_A denotes the label of authentication session that sender A has made. A is the sender's identifier which is denoted with the sender's certificate sequence. C is the identification of the receiver and is used together with IP address of the receiver. SMI denotes simple mail information and T stands for timestamp that TS generate for this mail message.

2) If there is any permission that is produced by the TS in a mail delivery proof, we should access the TS to form the evidence chain. The TS keeps all permissions of a mail delivery and we can abstract these permissions using SMI as index. According to permission format described in step 1, we can find the two mail servers that participate in the mail delivery procedure with identifier A and C. Here A is the node with non-repudiation service function. If permission is in format 1, then node A is the sender. If permission is in format 2, then node A is the receiver. Therefore we can find out all nodes that participate in a specific mail abnormal delivery. Furthermore, it is easy to find out the starting point where the normal or abnormal delivery mode starts.

3) We extract permissions from the nodes that participate in this mail transfer in abnormal delivery mode using SMI. We verify these permissions and compare them with those permissions stored on TS respectively. If these permissions pass verification and are exactly the same as those permissions stored at the TS, we can confirm that the corresponding nodes transfer mail message in abnormal delivery mode and find all break-points of evidence chain. Moreover, because each permission contains timestamp information, we can determine the order of nodes who forwarded mail message in abnormal delivery mode. For a specific email transport procedure, we

connect its abnormal delivery sender node, TS and abnormal delivery receiver node together. Otherwise, we can find corresponding normal delivery proofs with SMI. Finally, we obtain a new evidence chain for a mail delivery through normal delivery proofs-permissions-normal delivery proofs.

An abnormal delivery procedure consists of 4 stages including authentication, interactive inquiry, abnormal delivery permission and mail transport statement. Two situations could happen with abnormal delivery mode, one is called abnormal sending mode (Fig. 4) and the other is called abnormal receiving mode (Fig. 5).

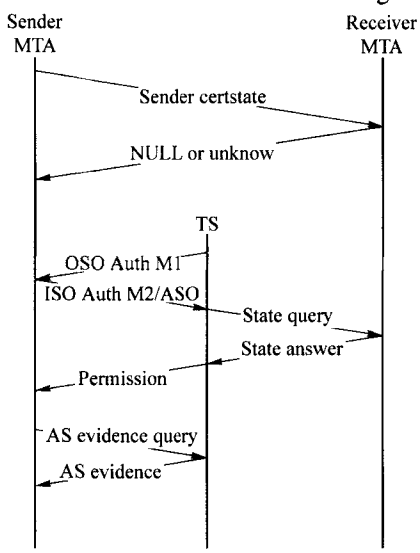

Fig. 4 Message sequence of abnormal sending mode

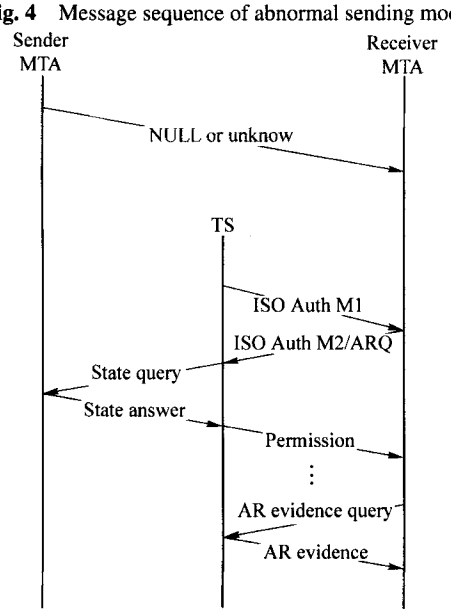

Fig. 5 Message sequence of abnormal receiving mode

Similar to normal delivery mode, authentication is carried out with ISO/IEC 9798-3 protocol. Messages ISO Auth M1 and ISO Auth M2, as shown in Figs. 4–5, are messages for authentication.

The TS inquires a node's interaction party using interactive inquiry mechanism. The TS inquires the interaction party whether it is a node with non-repudiation module installed and determines whether the TS should grant the node permission of abnormal delivery. Messages state query and state answer, as shown in Figs. 4–5, are messages for interactive inquiry.

There are two pieces of messages in abnormal delivery permission stage. One is an abnormal delivery request which the node with non-repudiation module sends to the TS. The other is an abnormal delivery permission or refusal that TS send to this node. In contrary to permission, the MTA, which has received this refusal, must transfer mail in normal transport mode. The TS sends either a permission or refusal depending on the outcome of the interactive inquiry stage.

There are two pieces of messages in mail transport statement stage. One, namely the AS or AR evidence query in abnormal sending or receiving mode respectively, is a abnormal delivery statement request that the node with non-repudiation module sends to the TS. The other one, namely the AR or AS evidence in abnormal sending or receiving mode respectively, is an abnormal delivery statement that the TS sends to the initiator.

The TS and the MTA store all three kinds of proofs including permissions or refusals, abnormal delivery statement requests and abnormal delivery statements in evidence library to inspect a mail abnormal delivery procedure. If the MTA fail to pass authentication by the TS, the TS should suspend sending to the MTA permission or refusal until it receives the MTA's retransmission message after a certain timeout period expires. If the MTA fails to pass authentication because the TS can't receive the correct authentication from the MTA within a given time, TS should terminate the current interaction session.

If the MTA cannot receive permission or refusal from the TS within a certain time period, the MTA should send the TS abnormal delivery request again. If the MTA doesn't receive a piece of permission or refusal after it has retransmitted the abnormal delivery request a certain times, the MTA will terminate this mail transmission and maintain the current status for latter retransmission.

If the TS cannot receive abnormal delivery statement request within a certain time, the TS will retransmit permission or refusal message. If the MTA does not receive the permission or refusal after the TS has sent the information three times, the TS should terminate the session and record this failure. If the MTA cannot receive the abnormal delivery statement within a certain time, the MAT should retransmit the abnormal delivery statement request. If the MTA does not receive the abnormal delivery statement after it has retransmitted the corresponding

request three times, the MTA should terminate this interactive session and record this failure.

4 System design and implementation

Based on the NRPUM protocol and other security mechanisms, we have implemented an email system with non-repudiation services according to the description in Section 3.

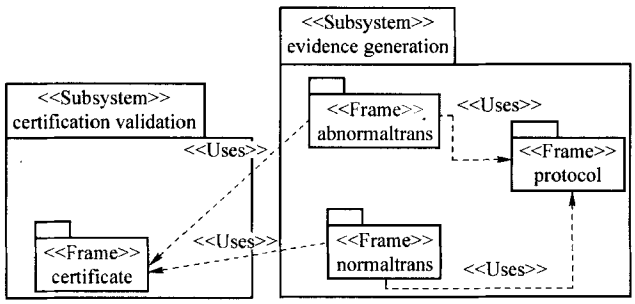

Fig. 6 System package diagram

As shown in Fig. 6, the email delivery system with non-repudiation service consists of two components: certificate validation subsystem and evidence generation subsystem. The former subsystem includes one package called certificate and the latter subsystem consists of three packages including NormalTrans, AbnormalTrans and Protocol.

The certificate validation subsystem verifies certificates and provides valid certificates for evidence generation and evidence management.

Evidence generation subsystem generates valid non-repudiation evidences using the valid certificates that are generated by the certificate validation subsystem. Specifically, the operational procedure is as follows.

Step 1 parties exchange certificates to insure that each node obtains a valid certificate of corresponding interactive entities.

Step 2 an authentication protocol is executed to make sure that both sides are the owners of corresponding certificates.

Step 3 the NRPUM protocol is executed to produce chain of evidence that can affirm the delivery procedure for a specific mail, finally the subsystem store all these evidences in evidence library.

5 Testing and verification of the email delivery system

We have established a testing environment which consists of 5 hosts. Two hosts work as the UAs. The sender UA has an IP address of 192.168.1.21 and the receiver UA has an IP address of 192.168.1.154 respectively. Both UAs are installed with DLL for non-repudiation module, UA secret key, UA certificates, corresponding server's certificate and TTP's certificate. Two hosts work as mail servers, with names of test.buaa.edu.cn and rcpt.buaa.edu.cn respectively. Both mail servers are mounted with DLL for non-repudiation modules, mail server's secret keys, mail server's certificates, corresponding UA's certificate and the TTP's certificate. The IP addresses for the mail servers are 192.168.1.248 and 192.168.1.249 respectively. We installed a TTP service program and a TS service program to build a TTP and TS server. Both the TTP and the TS hold a secret key, a certificate and the corresponding certificates for UAs and mail servers. The fifth host works as a CA with IP address of 192.168.1.247. All five hosts are mounted with a database respectively.

To verify the non-repudiation service of our email delivery system, we test and verify the system with mail normal delivery, mail abnormal delivery and others complex cases. In all cases, each host holds the corresponding interactive party EOO and EOR respectively.

Figures 7–8, respectively, are two screen snapshots of proofs that sender UA and the corresponding interactive MTA hold after a specific mail normal delivery procedure.

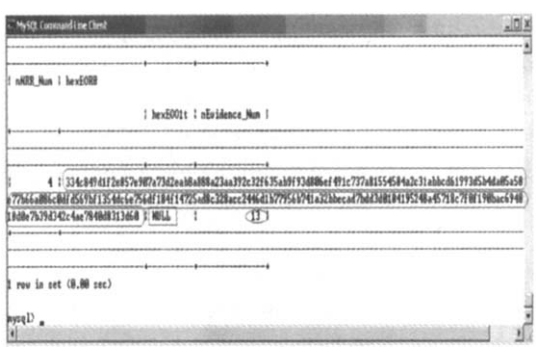

Fig. 7 EOR of mail server test.buaa.edu.cn that sender UA holds

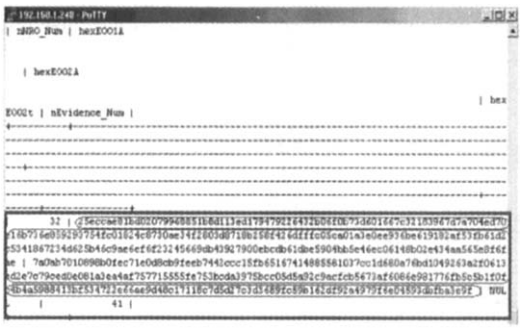

Fig. 8 EOO of sender UA that mail server test.buaa.edu.cn holds

In Fig. 7, the information marking with rectangle is hexadecimal EOR of the mail server test.buaa.edu.cn that sender UA holds. Similarly, in Fig. 8, the information marking with rectangle is hexadecimal EOO of sender UA that the mail server test.buaa.edu.cn holds. All proofs consist of messages of the NRPUM protocol and the content of the mail that is being delivered. These proofs are signed with secret keys of entities which generate the proofs. For instance, the EOR which is described in Fig. 7 is signed with the secret key of the mail server test.buaa.edu.cn and the EOO in Fig. 8 is signed with the secret key of the sender UA. Evidences are digests of the information including entities of the mail delivery, the mail delivery time and the mail content etc. With these evidences, no party along the mail route can repudiate. Because each party of a specific mail delivery holds non-repudiation proofs of corresponding interactive entities and all proofs of the specific mail delivery can form an evidence chain with SMI as index, neither the sender nor the receiver can deny a specific mail delivery.

6 Conclusions

In this paper, we describe the design and implementation of an email delivery system with non-repudiation services. First, we present design goals for our system. According to the system goals, we analyzed the key points to accomplish the non-repudiation service of the mail delivery. Second, we present solutions for forming evidence chains and achieving protocol backward compatibility. Finally, based on the NRPUM protocol, we implement an email delivery system with non-repudiation services. Through testing and verification, we demonstrate that the system can be compatible with standard protocols such as SMTP and POP3 and the system can provide non-repudiation service to mail delivery procedures. The use of this system and relative techniques can help in tracing the mail delivery path, and thereby can help in defending against spam Emails.

Acknowledgements This work is supported by the Defense Fundamental Research Program of China, and the Co-Funding Project of Beijing Municipal Education Commission (SYS100060412).

References

1. Otis D. Internet-Draft, MASS impacts upon reputation 2005
2. RFC 2015, MIME Security with Pretty Good Privacy(PGP). 1996
3. Crispin M. RFC3501. Internet message access protocol version 4 rev1. 2003
4. Even S, Goldreich O, Lempel A. A randomizing protocol for signing contracts. Communications of the ACM, 1985, 28(6): 637–647
5. Abadi M, Glew N, Horne B, et al. Certified email with a light on-line trusted third party: Design and implementation. Proceedings of the 11th international conference on World Wide Web, May 07-11, 2002, Honolulu, Hawaii, USA. ACM Press,2002: 387–395
6. Bahreman A, Tygar D. Certified electronic mail. In proceedings of the internet society symposium on network and distributed system security (NDSS 1994), Internet Society. February 1994, San Diego, CA, USA. IEEE Press, 1994: 319
7. Micali S. Simple and fast optimistic protocols for fair electronic exchange. Proc. of 22th Annual ACM Symp. On principles of distributed computing (PODC'03), July, 2003, Boston,MA,USA. New York, NY, USA:ACM Press, 2003: 12–19
8. Gomila L F, Capella M P, Rotger L H. An efficient protocol for certified electronic mail. Information security workshop (ISW'00), December 20-21, 2000, Wollongong, NSW, Australia. LNCS1975, Springer-Verlag, 2000: 237–248
9. Xia Chun-he, Liu Cui, Li Xiao-jian, et al. Research and implementation of the non-repudiation protocol for email transmission between UA and MTA. Journal of computer research and development, 2007, 44(2): 236–241
10. Klensin J. RFC2821. Simple mail transfer protocol 2001
11. Myers J G, Rose M T. RFC1939. Post office protocol–version 3. 1996

Biographies: WEN Dan-yan, Ph. D. Candidate in School of Economics and Management, Beihang University, interested in the research on digital right management.

TONG Cheng-gang, M. S. in Key Laboratory of Beijing Network Technology, Beihang University, interested in the research on network security.

XIA Guo-ping, professor at School of Economics and Management, Beihang University. His research interests include BPR, MIS and DSS.