A Notarization Authority for the Next Generation of E-Mail Systems

Hiran Ekanayake, Kasun De Zoysa, Rasika Dayarathna

Department of Communication and Media Technologies,
University of Colombo School of Computing,
35, Reid Avenue, Colombo 7, Sri Lanka.

E-mail: hbe@ucsc.cmb.ac.lk, kasun@cmb.ac.lk, rasika@cmb.ac.lk

Abstract

Current email system is at a risk of loosing its demand because of its abuse. These abuses are ranging from receiving unsolicited emails to email frauds or repudiations. This paper discusses better approaches to overcome those limitations up to some extent with the concept of a trusted third party called email notarization authority.

Keywords: Secure Electronic Mail, Notarization Authority, Timestamping

1 Introduction

Electronic mail now has become the state of the art in distant communication. Its fancy is in its ease of use and cheapest cost. As a few years ago, one of the potential weaknesses with this service was its inability to provide a good security framework. But over the years there was a big effort to fix this problem and as a result now this service has a rich security infrastructure based on public key infrastructure [1].

However, email users are facing various other problems while using this service. There are lots of nuisance emails appearing on mailboxes daily. In other hand, emails have become the carrier for electronic viruses. Also once you get an email you cannot be assure that the actual sender of that email is the one who appearing on the "from" field of the email. Again, the current email system is unable to provide any legal proof for any party involved in an email transaction. As a result, current email system is loosing its strength to provide a secure, reliable and trusted communication channel for today's information exchanges [2].

Therefore, to stay with this service in the future, a more work has to be carried out in order to fix these weaknesses. Our new approach, which is based on a notarization authority, can solve most of the e-mail security issues relating to repudiation such as when an email is created, who created it, when it was sent, was it delivered to the intended recipient, was it observed by the recipient.

2 Potential Solutions

There are different appearances for email systems: POP mail, and web mail. In addition, mail clients are differing as MIME [3] compatible, and S/MIME [4] compatible. Despite, email differs in various other ways: corporate mail, and other, all these together provide users the ability to exchange information with or without various contexts: security, reliability, ease of use, cost, etc.

Over the years several attempts have been made to increase the reliability of this service. For instance Outlook Express [5] allow read receipts to provide an indication of guaranteed delivery to its users. However, it has fallen to provide the requested service, because the recipient can ignore to send a receipt.

Under digital notarization concept, your email will be digitally timestamped, and later you will have a legal proof for your email transaction. These proofs vary from sending to reading of an email. ReadNotify [6] is a leading example in this area. There is no need to have client side plug-ins or any other modules to use ReadNotify notary service and they track the recipient(s) in a very transparent way. To receive the services from ReadNotify one has to register, and from that point onwards emails arrive by this address become eligible to receive the service. There are some other notary services, which enable similar functionality. However, none of them have not yet able to provide a comprehensive framework for strengthen the email system.

3 Role of the Notarization Authority (NA)

This section presents a discussion on how to expand the capabilities of the digital notarization to solve the repudiation issues with regard to email transactions. In order to solve these issues we proposed a trusted third party called "Notarization Authority" with the following capabilities.

- **Email Time stamping**: prevents backdating the existence of an email.
- **Proof-of-Posting Certificates**: provide legally acceptable evidence to prove that you actually posted an email.
- **Guaranteed Delivery**: will ensure that your email is delivered to the intended recipients; and after delivering you will be informed with a digital receipt.
- **Proof-of-Observing Certificates:** provide legally acceptable evidence to prove that your email is opened or read by the intended recipients.

3.1 Proof-of-Posting Certificate

This certificate proves that you have sent an email at particular time. Two different scenarios were used.

Scenario 1: The sender is a registered entity under the notarization authority. For each email send by the sender, a copy will be sent to that authority. Later the sender will receive a proof-of-posting certificate. Figure 1 illustrates this scenario.

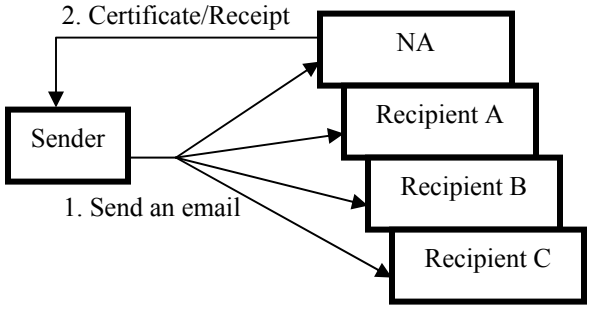

Figure 1: Proof-of-Posting Certificate Scenario 1

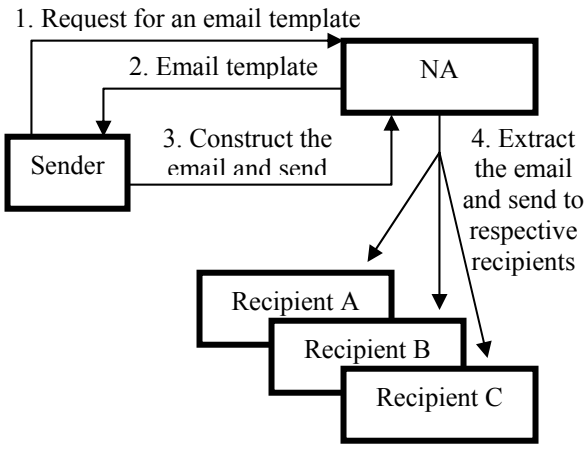

Figure 2: Proof-of-Posting Certificate Scenario 2

Scenario 2: The sender is a registered entity under a notarization authority. As the first step the sender requests a template from a notarization authority. Notarization authority responds by sending back a registered time stamped template. Based on this template the sender constructs his message, appends attachments, puts recipient email addresses, and finally sends it back to the authority. Notarization authority will then verify the template and extract the absolute email message from this filled template. This absolute message will be sent to the intended recipients. Figure 2 illustrates this scenario.

3.2 Proof-of-Observing Certificate

This certificate proves the actual observation of an email. Observation (reading) is somewhat difficult to capture. The following scenario describes how this event is captured using some existing technologies that works for both POP and web mails as well.

Scenario: The sender is a registered entity under a notarization authority. As the first step the sender sends email which need the proof to this authority. Notarization authority will then extracts the absolute message and encapsulates this message into a password protected zip file and send this email under a new envelope to those respective recipients with instructions on how to proceed. Each recipient has to go through these instructions, and has to visit the authority's dedicated website to get the password to unzip the file back to the original email. This successful password-transferring event will be captured as the evidence of reading the email and a proof-of-observing certificate will be issued. Figure 3 illustrates this scenario.

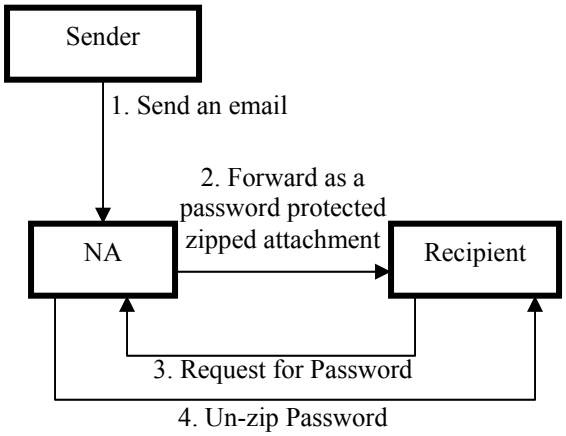

Figure 3: Proof of Observing Certificate Scenario

3.3 Spam Mail Prevention

With some few enhancements our notarization authority can be configured to filter Spam mails. Here it is assumed that all trusted email addresses are registered under the notarization authority. This authority has a mechanism to validate those email addresses and their respective owners periodically.

Scenario: The recipient is a registered entity under a notarization authority and this authority has a database of trusted email addresses. A filter protects the recipient's email client and configures to bypass emails only from trusted sources. All un-trustable emails will be forwarded to the notarization authority. The authority will then validate the respective sender against its trusted address database and forward back the emails with a report attached. Based on this report recipient's email filter may decide whether to drop it or not. Figure 4 illustrates this scenario.

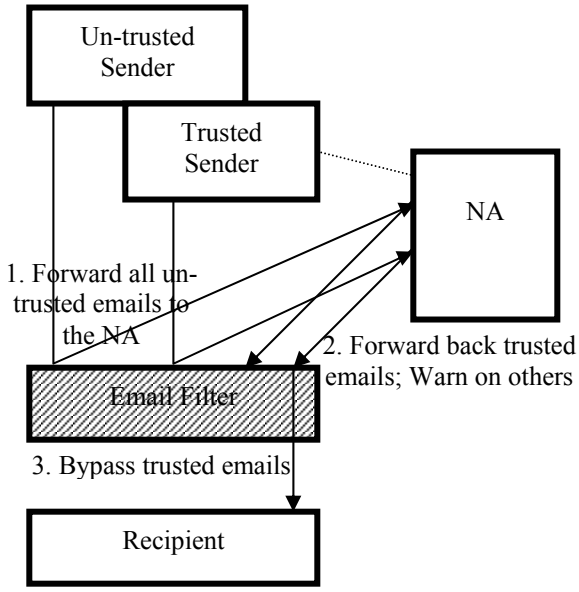

Figure 4: Spam Mail Prevention Scenario

4 The System Architecture

This section describes the system architecture with the design aspects. As illustrated in Figure 5 the system is divided into two sub-systems:

- **The Web-based Service**: provides services to the users
- **Notary Server**: executes periodic functions and security intensive functions

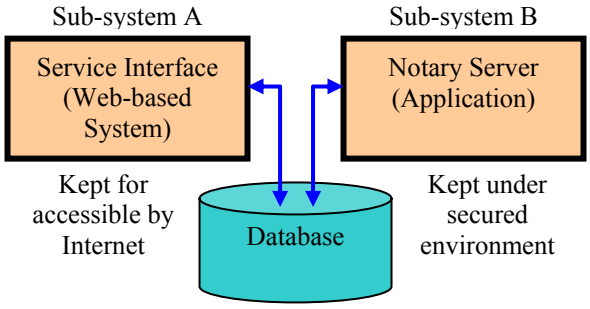

Figure 5: Sub-Systems of the Main System

The database acts as a common gateway to these two sub-systems and separates the two into two different functional domains.

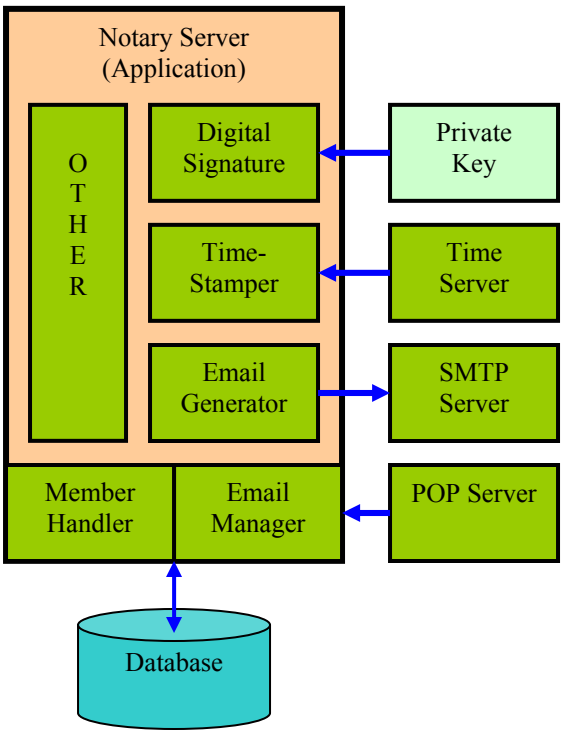

Figure 6: Notary Server Sub-system

The notary server is the hart of the system. It is to be kept under a secure environment, and its main purpose is to execute periodic functions that need some higher degree of security. These functions includes:

- **Email Handling**: both sending and retrieving
- **Time-Stamping**: synchronizes the time with a remote time server and provides time stamping service to certificates and receipts.
- **Issuing Proof-of Certificates**: construct digitally signed proof-of-posting and proof-of-observing certificates for those applicants.
- **Member Registration**: validates new member registrations and periodic verification of information**.**
- **Message Handling**: feature extraction from email messages, enveloping and email constructions.

Figure 6 illustrates components of the notary server sub-system where these functions are executed.

The Web service sub system offers the following services:

- **Web-mail & Message Templates**: web mail offers the facility to construct emails without using a separate mail client. Message template differs according to the purpose of the sender. For instance, if you need to send a birthday greeting email on a pre-determined day you have to use a greeting message template.
- **Email Status**: offers the facility to query the current status of an email.
- **Certificate Issuing Facility**: takes the information from requester and sends a proof-of certificate.
- **Certificate validation facility**: validates any issued certificate.

Figure 7 illustrates components of the web service sub-system where these functions are executed.

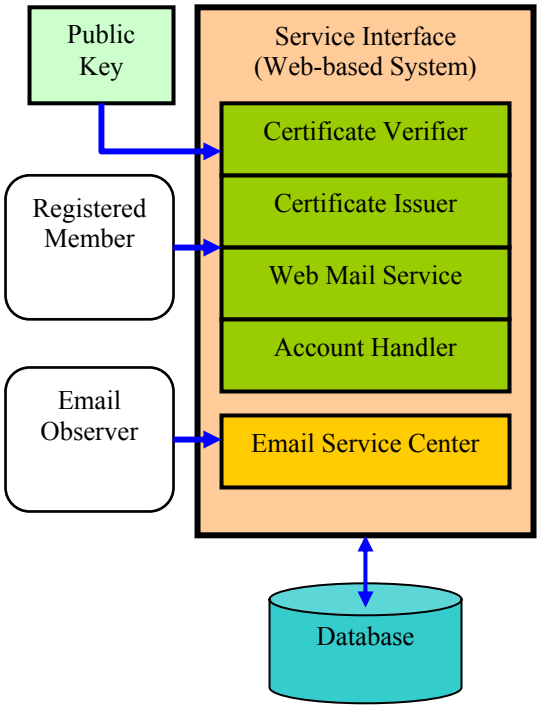

Figure 7: Web Service Sub-System

5 Conclusions and Future Works

5.1 Conclusions

This paper described some methods to make the existing email system a much perfect one based on existing technologies and standards. Several initiators have already built notarization authorities for emails using their own approaches. However none of them provide a complete solution. This is because current email protocols such as SMTP and POP [7] do not provide significant messages for such enhancements.

However, our proposed notarization authority enriches in facilitating non-repudiation and Spam mail filtering. These methods will be useful for designing a better email system for the next generation.

5.2 Future Works

Email tracing facility is not incorporated into the system yet. If the tracing facility required the sender could get the status information on how an traveling with the location and time information. So he can visualize the current residence of any email.

Some extensions to the email, for instance blocking or forwarding, are very easy to implement in the system. For example, the email forwarding can be done in the following manner:

- **Direct forwarding**: forwards an email to someone else other than the recipients mentioned in the email.
- **Cluster forwarding**: forwards single email to a group of recipients.
- **Chaining**: If the email can't reach to the recipient A then forward it to recipient B; if that attempt also failed then forward it to recipient C, and so on.

References

[1] "Cryptographic Message Syntax Standard", Public-Key Cryptography Standards, RSA Laboratories, [Online] Available at http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html

[2] Rasika Dayaratna, Kasun De Zoysa, "An Enhanced Security Mechanism for General Purpose Email Clients", International conference on Computer Communication, The International Council for Computer Communication, Mumbai, India, August 11-14, 2002

[3] "MIME related links", Multipurpose Internet Mail Extensions MIME, [Online] Available at http://www.oac.uci.edu/indiv/ehood/MIME/MIME.html

[4] "S/MIME Version 3 Message Specification", Request for Comments, [Online] Available at ftp://ftp.ietf.org/rfc/rfc2633.txt

[5] Microsoft Outlook Express, Microsoft cooperation, [Online] Available at www.miccrosoft.com

[6] ReadNotify notary service, [Online] Available at http://www.readnotify.com

[7] Rolf Oppliger, "Security Technologies for the World Wide Web, Artech House Inc., 2000