A Secure Protocol for Delivering Electronic Documents via a Third Party

Bassam Al-Hammadi, Ph.D.
Compute Programs
Institute of Public Administration, Riyadh

Abstract - To validate a transaction between any two parties, an independent third party witness is required to sign and approve the undergoing transaction. A transaction may include important documents, such as, digital identifications, certificates, contracts, secure documents, emails, bills, receipts, and notices. The exchange of these documents through the Internet has become an essential business need. This paper discusses a protocol for fair exchange of electronic documents via a third party to protect both the sender and the recipient from any possible repudiation by any of the communicating parties. The protocol can be implemented on the existing Internet infrastructure using the email protocols.

1. Introduction

Nowadays, network security is an important issue in any application that employs networks to transfer data. Packet switching networks, such as the Internet are in a real need for comprehensive solutions to their security problems. These problems are due to the fact that data packets (data units) in the Internet are handled by many intermediate networks and devices, where anyone can access them.

In general, These security problems can be divided into four overlapped areas: Cryptography, Integrity, Authentication, and Access control [1]. Access control is concern with authorization, rights, and privileges, which is not related to the subject of our paper. The other three areas will be discussed briefly in the following sections.

1.1 Cryptography

Cryptography is concerned with keeping communications private. It is a science for scrambling information. The main concept of cryptography is based on two algorithms: Encryption and decryption. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption; it is the transformation of the encrypted text back into the original text [2].

Encryption and decryption require the use of some secret information known as a key. Depending on the encryption algorithm used, the same key might be used for both encryption and decryption, and this is known as Secret key or symmetric key cryptography. Secret key cryptography is based on a single key that only the sender and the recipient possess. The sender and recipient should keep the key in a secure place.

In other algorithms, the keys used for encryption and decryption might be different, such as, public key cryptography. In 1976, Whitfield Diffie and Martin Hellman introduced the concept of public key cryptography. In their concept, each person gets a pair of keys, one called the public key and the other called the private key. Each person's public key is published while the private key is kept secret. Practically, the two keys are generated so that it is impossible to obtain the private key known the public key of any person. Therefore, the need for the sender and receiver to share the same key (as in secret key cryptography) is eliminated [3].

1.2 Integrity

The integrity of the transmitted information is another important network security issue. This part of network security checks whether the received message has been altered or the sender is not the real originator of the message. One way hash functions and digital signatures are methods for integrity verification.

Digital signature guarantees the message integrity. To generate the digital signature, first a one way hash function transforms a variable-size input message and produces a fixed-size output string, which is called the message digest. The message digest represents a unique "fingerprint" of the message. Given the message digest it is impossible to guess the original message. In addition, there are no two messages that have the same message digests [4].

Then the message digest is encrypted using the private key of the originator and is appended to the message. The recipient will use the public key of the originator to decrypt the message digest and recalculate the message digest of the received message. If both

message digests (one generated by originator and the second generated by recipient) are equal, then the integrity of the message is verified, otherwise the message has been altered.

Digital signature is like a handwritten signature but in electronic form. The digital signature is a piece of data that assures that a named person wrote the message. A digital signature of a message cannot be repudiated; the signer of a message cannot later deny it by claiming the signature was forged. In other words, digital signature enables "authentication" of a digital message, assuring the recipient of a signed digital message of both the identity of the sender and the integrity of the message [4].

1.3 Authentication

Authentication is the process of identifying a user, usually based on a username and password. Authentication ensures that the user is who he or she claims to be, but it does not provide anything about the access rights of that user. Most computer security systems are based on a two-step login process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity [1].

1.4 Digital Certificates

Digital certificates, also called digital IDs, digital passports, or public-key certificates, are defined by the International Telecommunication Union (ITU) standard called X.509. A certificate establishes the user's identity including his/her public key. Servers may grant access only to clients with valid certificates, and clients may trust servers with certain certificates [5].

Digital certificates are issued by Certificate Authorities (CAs). A CA is a trusted third-party organization or company. The role of the CA is to guarantee that the user who granted a unique certificate is who he/she claims to be including his/her public key. This means that the CA needs a document from a trusted institution, such as a driver license, credit card, or social security identifications, to confirm the user identity. The CAs are critical components in network security, because they guarantee that the two parties exchanging information are really who they claim to be [5].

The CA makes its own public key available through the Internet. The recipient of an encrypted message uses the CA's public key to decrypt the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply [5].

Digital Certificates are kept in network directory services for public access. The directory services maintain databases to retrieve certificates upon requests. A common specification of directory services is known as X.500 [6]. Directory services are expected to form the basis of certificate distribution mechanisms, and the backbone of a worldwide PKI (Public Key Infrastructure) [6].

2. ELECTRONIC MAIL

Email has become one of the most important Internet applications in our daily lives. It has many advantages over the postal mail (paper-based mail). In contrast, Email has faster delivery with no regards to the distance or the place of the originator and the recipient. Therefore, email tends to replace some of the paper-based postal mail services with more efficient and advanced services. In order for the email systems to do the job right, security and protection must be employed in a broader range, especially for those services that require special delivery.

Email systems went through many developments and enhancements. Two decades ago email started as a simple file transfer protocol. Then a lot of protocols and standards were proposed to fulfill the huge demands for this service. The first proposal was in 1982 by ARPANET in form of two standards. One was for the transmission protocol (RFC822) and the other one was for message format (RFC822) [1].

In 1984, the CCITT (Consultative Committee on International Technology and telephony) announced its recommendations X.400, which defined general store-and-forward messaging services. In 1988, the CCITT updated the X.400 recommendations to include security services to protect messages against modification and disclosure, and to allow communicating parties to authenticate their identities. The X.400 was redesigned to work over the OSI communication stack [7]

Internet email system consists of two major components: User Agent (UA) and Message transfer Agent (MTA). UAs are local programs that allow users to send, receive, and manipulate messages through commands or menu driven interface. MTAs are system daemons that transfer message from the UA of the sender to the UA of the recipient [2].

The Simple Mail Transfer Protocol (SMTP) provides inter-machine email transfer services. It is the de facto protocol used by nearly all MTAs on the Internet. The UA communicates with the local MTA on behalf of the user to request message transfer. Then the local MTA communicates with a remote MTA on the destination system, or one on an intermediate relay, as shown in Figure 1. Most MTAs support store-and-forward features to ensure that those messages not delivered to the next hop can be retransmitted later on [2].

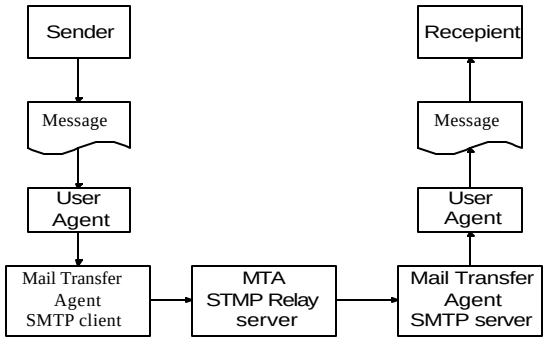


Figure 1. Internet Email Architecture.

3. The Protocol

In postal mail, it is practical to send a certified mail. First, the originator fills a request for certified mail. Then, at the destination, the postman asks the recipient to sign the certificate before delivering the letter to the recipient and then the postman sends back the signed certificate to the originator. In this case the postman is trusted by the originator to get the signed certificate from the recipient, and the recipient is trusted the postman to deliver the correct mail. Therefore, a trusted third party (the postman in the postal mail situation) is an essential issue during the delivery process [8].

Unfortunately, the postal certified mail delivery scenario is impossible to be implemented in the existing email systems without employing a trusted third party, because when originator sends the message, there is no guarantee that the recipient will acknowledge the received message. Generally, email has security violations, and repudiation is one of these violations. Repudiation is the denial of events by one or more of the communicating parties [9].

The denial of an event can be in one of the following shapes [9]:

- denial of receiving a message
- denial of sending a message
- denial of the sending time or receiving time
- denial of message content by the originator

Non-repudiation is the prevention of the denial by providing a proof of the events from the communicating parties certified by a trusted third party. The protocol is designed to provide the required proofs for both the originator and recipient against any of the above denials. Moreover, the protocol infrastructure will be an extension that can be integrated easily into the existing Internet email standards. The protocol employs a trusted third party to help solving the problem of physical exchange of the messages and to provide the proof of delivery from the recipient.

This protocol consists of four main elements: a trusted third party which is represented by the Email Office (EO), the originator, the recipient, and the communications medium. The EO is a third party server that provides the email handling service in an electronic manner. The EO can play one of two different roles during the handling process of the email:

1) Active role: the EO has a direct access to the the content of the message.
2) Passive role: the EO can not access the message.

The protocol implements the passive role of EO. The EO will include the message digest in the proof of delivery for any future dispute. In this way, the EO will not brake the privacy seal of the message and eliminate the need for a huge secure database for all the transactions, because EO can verify his signature on the receipts. Also, the communicating parties do not need to worry about the security and privacy of their messages.

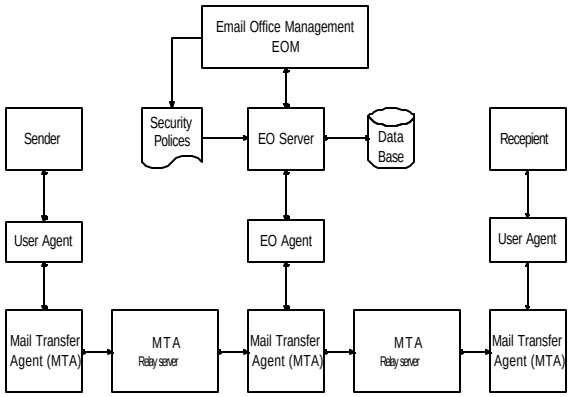
From now on, we will use Alice and Bob instead of the originator and the recipient respectively. Both Alice and Bob should have a public-private key pair with certificates from a well-known CA. The protocol is designed based on the worst case scenario, where both Bob and Alice act unfair. For example, one of them may repudiate an action taken by the other.

The communication medium can be any network environment, such as the Internet. The Internet is an insecure heterogeneous network, where messages can be accessed and maybe changed by any user in the Internet. Also, there is a possibility that the message misrouted or even lost in the network.

Figure 2 shows the integration of the EO to the existing Internet email architecture. The EO is considered as a regular end user that has a UA and MTA to receive and transmit certified email and proof forms. The EO consists of four components: Email Office Management (EOM), EO Server, Database, and Security Policies. The EOM controls and monitors the EO Server and establishes and updates the Security Policies for the EO. The EO server implements the Security Policies to process request for secure document delivery and uses the database to save those messages that are in a waiting state for delivery. Another part of the Database is used to keep receipt of delivered email for certain time as stated in the Security Policies for future disputes.

The basic principle of the protocol is to simulate the real life post office certified mail with a practical solution to the problem of exchanging the email and the receipts at the delivery instance. For example, when Alice wants to send a certified email to Bob, she needs to fill up one of the EO forms for this service and sign it. Alice encrypts the message with Bob's public key (like putting the letter in an envelope) and includes Bob's address in the form and the message digest of the

message. It is optional to write the subject of the email



in the form.

Figure 2. The EO Integration in The Internet Email.

Now Alice can send the encrypted message to the EO along with the signed form. The EO will send the form to Bob not including the message. If Bob accepts to receive the email, he will sign the form and send it back to EO (Note, Bob has not received the message yet). When the EO receives the signed form from Bob, EO will sign the form and include the email message with it and send it to Bob. Thereafter, the EO will send the same form to Alice (Note the form is signed by Alice, Bob, and the EO) as a proof of delivery.

4. Protocol Implementation

The implementation of the protocol has three phases: message preparation, message distribution, and proofs distribution.

4.1 Message Preparation

Alice should request the Certified Email Form (CEF) from the EO through the following operations, each operation represents a transaction in Figure 3:

1) Alice fetches the public keys (Certificates) of both the EO and Bob from a Network Directory.

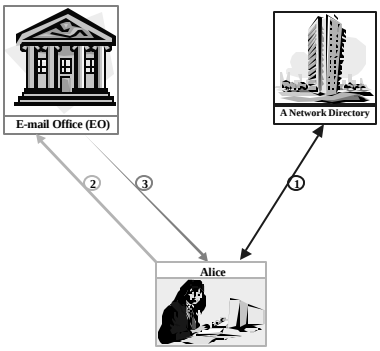
2) Alice encrypts a request R for a CEF with her private key, then encrypts it with the EO's public key (Alice's certificate is included in the encrypted message for future use by the EO) and sends the request to the EO.

3) The EO encrypts the CEF with his private key, then encrypts it with Alice's public key (the EO uses the public key from Alice's certificate) and sends it to Alice.

4.2 Message Distribution

This phase is represented in the transactions of Figure 4:

1) Alice applies a one way hash function to the message to produce the message digest then encrypts the message digest with her private key to produce the message signature. Then concatenates the original message with the message signature and compresses the output. Now Alice needs to encrypt the compressed output with a secret key K_A generated by her. Then the secret key is encrypted by Bob's Public key. She fills the CEF and includes the message digest in the CEF then signs the CEF (by producing the digest and encrypts it with here private key) and includes the unsigned CEF and the message digest. Finally, she encrypts the signed



CEF and Bob's signed message with the EO's public key then sends it to the EO.

Figure 3. Message Preparation Phase.

2) The EO Decrypts the received message and signs the CEF. Then the EO sends only the signed CEF (excluding the encrypted message) to Bob by encrypting it with Bob's public key.

3) Bob decrypts the email and reads the CEF, in order to receive the message he should sign the CEF and sends it back to the EO. Bob also keeps a copy of the CEF to proof that the EO will deliver a message from Alice.

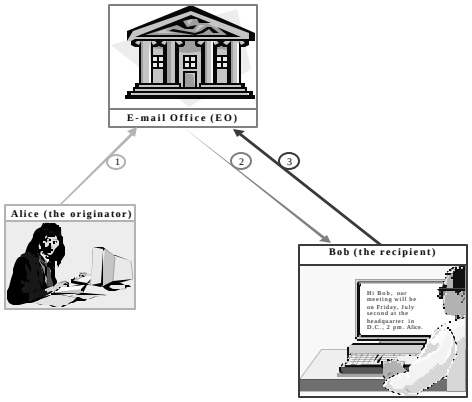


Figure 4. Message Delivery Phase.

4.3 Proofs Distribution

In case Bob accepted the CEF and signed it, the EO will send the signed message to Bob, and a receipt (which is the signed CEF) to Alice. Otherwise, if Bob refused to receive the message within a specific time, the EO will send a proof of undelivered message to Alice.

5. CONCLUSION

Many communicating parties over the Internet are in a need for secure document delivery to verify the delivery of their messages, and to take the right actions in case the recipient did not receive the message. This paper presents a protocol that provides the proofs that are needed for exchanging secure documents. The protocol implementation is an extension of the existing email protocols. This protocol's key element is the email office, which is the trusted third party that provides the delivery services without breaking the privacy seal of the delivered message. Digital certificates, digital signature, and session key are used to ensure authentication, privacy, and integrity of the delivered messages. Also data compression is used for space and speed improvement.

REFRENCES

[1] Tanenbaum S. Andrew, Computer Networks. Prentice Hall, Inc., Upper Saddle river, New Jersey, 1996.

[2] Hughes Jr. Larry, Actually Useful Internet Security Techniques. New Riders, Indianapolis ,1995.

[3] Kaufman. C., Perlman R., and Speciner M., Network security, Englewood Cliffs, NJ, Printice Hall, 1995.

[4] R.L. Rivest, A. Shamir, and L.M. Adleman.A method for obtaining digital signature. Communications of the ACM, pp. 120–126, February 1978.

[5] CCITT Recommendation X.509: The Directory — Authentication Framework. 1988.

[6] CCITT. Recommendation X.500: The Directory — Overview of Concepts, Models and Services. 1988.

[7] S. Radicati, Electronic Mail: An introduction to the X.400 Message Handling Standards, McGraw-Hill, Inc., New York, 1992.

[8] Coffey T, Saidha P, Non-repudiation with mandatory proof of receipt, Computer Communication Review.

[9] Zhou J., and Gollmann Dieter G., A Fair Nonrepudiation Protocol, IEEE, pp. 55-61, 1996.

Biography

Bassam A. Al-Hammadi (hammadib@ipa.edu.sa) received a Ph.D. in computer Engineering from Florida Tech, Melbourne, USA, in 1999. From 1993 to 1995 he was an instructor and A project leader of the LAN project at the Institute of Public Administration (IPA), The Computer Programs. Also, he was the program coordinator between 1999 and 2000. He is a member of the Computer Security Institute (CSI). Currently, he is a faculty member of the IPA. His main research interests are in the field of Information Security, Computer Networks, and Computer Architecture.