A Guide E-Mail Systems and Security

Brian Donadio

East Carolina University

Abstract

Electronic Mail is quite arguably the most important application for personal and business communication across the Internet. People depend on it for sending text, image and even sound files quickly to their destinations. This is a far cry from the Postal Service and even the Pony Express for delivering messages to their destinations in days or even weeks.

E-Mail was designed to be both easy to use and quick for fast end to end message delivery. Because of these factors E-Mail does not have many built in security measures by default. Barebones E-Mail services do not provide non-repudiation between the sender and receiver. They also fail at providing encryption to protect the clear text nature of E-Mail as it traverses the Internet.

The goal of this paper will be to provide secure methods of sending and receiving E-Mail over the Internet. This will include both server/provider technologies, as well as, end user client solutions to encompass E-Mail technology as a whole. E-Mail is a convenient technology that most people rely on for communication today, but it can come at a cost if poor security measures are taken.

Introduction

Electronic Mail is one of the most used tools when it comes to business and personal communication in the world today. Notes, Messages and even Pictures can be sent quickly from source to destination using E-Mail. The senders of these messages often assume that the contents are private and are kept sealed from the source to the destination. This is not always the case! With the proper techniques, malicious hackers and spammers can read and send unauthorized E-Mail information that senders and

receivers assume is private. This could range from reading/modifying a message being sent between E-Mail servers to sending unauthorized Spam messages to individuals throughout the world. The heavy reliance on E-Mail makes the proper security precautions essential to providing secure and reliable E-Mail solutions in organizations today.

Overview of E-Mail Systems

The E-Mail process can be broken down into two general parts, message sending and message delivery. The processes are dependent on each other to allow the E-Mail to be successfully set and delivered the correct destination. First, the message composition and sending process will be covered.

In this example a simple text message will be composed and sent to its destination. The end user's client E-Mail program plays what is known as the User Agent role [5]. Once a message is composed in an E-Mail client program, it sent to a SMTP server to be delivered to its destination. SMTP is Simple Mail Transfer Protocol as specified in RFC 2821 for delivering E-Mail messages and uses TCP port 25. In most cases an SMTP server is provided by an ISP or organization to provide E-Mail sending functions for an individual or organization. The E-Mail client computer first sends the SMTP server a "HELO" message to the SMTP server. This message informs the SMTP server that the client would like to send a message and even what type of message is being sent. If the SMTP server can accept the message, it will reply with a reply back to the client. Next, the client sends the "MAIL FROM:" message with the address of the sender. The SMTP server will then reply back with a "Sender OK" message to continue

the transaction. The destination address is then sent by the client with the "RCPT TO:" message. Once the Server replies back with the "Recipient OK" message the client can finally send the actual message. The "DATA" message is then send to the SMTP server followed by the text fields containing the message to be sent. The "QUIT" message is then sent and once this is confirmed by the SMTP server, the message has been sent as far as the client is concerned [11]. The message still has far to go before it reaches its final destination.

Once a message has made its way onto the Mail Server, it must be delivered towards the destination Mail Server. Mail Servers are identified by Mail eXchange entries in DNS. This is a special DNS entry that is held in DNS servers for delivering E-Mail. Mail Servers can play several roles in the transportation of E-Mail. Generally they play one of these two roles, Transfer Agent or Delivery Agent. Transfer Agents are responsible for transporting messages towards their final delivery destination [5].

The Transfer Agents use the DNS MX entries to route the message to its next hop on the way to the final destination. For example, if a message is destined for "mail.ecu.edu", the Transfer Agent may determine that it has to send the message to the TA at "ms1.google.com". This process can be repeated several times across several domains as the message makes its way towards the final destination. Eventually the message will arrive at its destination and the Mail Server will act as the Delivery Agent. The DA locates the appropriate mailbox for the user defined in the RCPT field of the message. The user can then retrieve the message from the Mail Server using one of several protocols such as POP3 or IMAP [5].

Common Vulnerabilities

As shown in the process detailed above, there can be many opportunities for hackers to send unauthorized messages, modify messages during delivery. Messages that are sent in clear text can be easily read if the mail delivery system is compromised. This could happen if MX entries are compromised or even with the installation of Rogue Mail Servers. When messages are sent to these compromised servers during the delivery process, the messages could easily be sent to alternate destinations along with the correct destination. This would allow hacker/spammers access to E-Mail addresses or sensitive information contained in the messages themselves.

Many of the problems that E-Mail users encounter are related to the material contained in messages that they receive. These sometimes include html formatted messages, harmful attachments or other forms of executable code. The most common and most known harmful E-Mails commonly contain viruses or malware. If these attachments are opened on a computer they can install viruses or spyware that can do anything from format the computer to sending an entire address books worth of viruses and personal information [10].

HTML messages also can be used to execute malicious code against a user. On some computers HTML messages are read with the same software used in web browsing which makes systems susceptible to the same vulnerabilities as those of the web browser. HTML messages that link to remote images can also reveal information about the reader. These images would be downloaded in the same way as browsing a website, allowing the remote server to collect information such as the reader's IP Address, time of message

reading, OS Type and Browser type. This may not seem like sensitive information, but in the case of outdated software, it could lead to uncovering vulnerabilities within the readers system. All of this would give the hacker/spammer a better chance of compromising a system or sending more items from spyware to plain old adware [10].

Security Requirements

For the purposes of this paper the main security goals are as follows. The E-Mail services must be able to provide Non-Repudiation and Encryption when necessary. A secure E-Mail system or client also must be able to minimize the effects of spam and malware on the systems that receive messages. The security measures analyzed here will be divided up primarily into two categories, first are options for end user or client based products; the second are server based or other corporate solutions. Methods of authentication will also be discussed to help provide identification of E-Mail users.

Client Based Solutions

E-Mail clients have traditionally used MIME (Multipurpose Internet Mail Extensions) for formatting most messages that have multiple messages embedded or for non-text based messages. Messages formatted in such a way are sent as clear text and as we know can be vulnerable to disclosing sensitive information to hackers and spammers [3]. The answer of course, is to provide encryption for important messages or even all messages sent if possible. There are many protocols that have been developed to encrypt and provide non-repudiation for E-Mail. Because these protocols were developed with particular goals in mind, it is important to choose the one that is most appropriate for the situation at hand.

The first encryption protocol to be discussed will be PGP or Pretty Good Privacy, one of the earliest and most popular encryption methods developed by Philip Zimmerman in 1991. PGP is a free encryption solution for encrypting E-Mail from between clients as many individuals need this type of service with E-Mail. Standard PGP addins support PGP/MIME, which is a very effective yet unstandardized protocol. This protocol combined the security built into MIME with the cryptostream properties of PGP [4]. PGP and PGP/MIME have been mostly abandoned for the newer OpenPGP.

OpenPGP is based off the same principles as the first PGP but is standardized and not backward compatible with PGP or PGP/MIME. OpenPGP uses MIME as the basis for formatting messages just as PGP/MIME does. OpenPGP uses Public Key Cryptography to encrypt its messages using a simple binary certificate created custom for OpenPGP. Messages encrypted in this format are encrypted using TripleDES (DES EDE3 Eccentric CFB). Once a user obtains a valid OpenPGP certificate, they can encrypt and decrypt messages using PGP addins for Outlook or other E-Mail client programs [7].

Another popular protocol for protecting E-Mail communications is S/MIME. Although it performs many of the same functions for E-Mail security as OpenPGP, the two protocols are quite different and therefore incompatible. S/MIME was developed by various vendors in the Information Technology industry and was formalized by IETF in S/MIMEv2. The IETF did not make S/MIME an official standard until S/MIMEv3 in 1999. S/MIME uses a similar yet different encryption scheme to that of OpenPGP by using TripleDES (DES EDE3 CBC) [7]. S/MIME uses Binary certificates based on

X.509v3 which require the user to have a certificate generated by a certificate authority before being able to use S/MIME functions. Although S/MIME has not been around as long as some forms of PGP, it is supported by default in many E-Mail client programs such as Outlook and Thunderbird [1].

It is important to note that both S/MIME and OpenPGP only encrypt the actual message and not message headers. If the entire message was encrypted, then it would have to be decrypted at each E-Mail server to read the sender and recipient information. Also, because both S/MIME and OpenPGP use public key cryptography to protect messages, a sender must have the recipient's public key prior to sending an encrypted message. Generally public keys are included with the certificate that clients use to sign messages. Once a message is sent to a recipient, they can accept the certificate of the sender thus storing the corresponding public key required to encrypt messages to that particular person. Although S/MIME and OpenPGP use different types of certificates, they are both able to sign messages with their corresponding certificate. This enables both protocols to provide authentication and non-repudiation for messages signed with certificates, ensuring parties can trust that they are communicating with who they think they are when conducting E-Mail communication [7].

Despite all of the scanning and filtering E-Mails endure as they make their way to be delivered at the final mailbox, malicious messages still get through. Many of these messages contain viruses or malware. Whether a user is a corporate user or personal E-Mail user, is important to have an anti-virus program that is able to identify harmful E-Mail attachments. Doing so can keep readers from opening many harmful E-Mails and

attachments, even if a message is opened by mistake. There are several anti-virus programs available ranging from free to very costly. One free option for personal E-Mail users is Avast! anti-virus. It provides Outlook E-Mail scanning in the default install.

Server Based Solutions

In many environments administrators or service providers prefer to have more control to provide services for E-Mail end users. As security requirements have grown, more vendors have developed server protocols and applications that provide various levels of E-Mail security. Server applications can provide virus protection, spam filtering, and even encryption. There are various types of setups that can provide these services and many of these possible solutions will be discussed in this section. One particular product that can work to provide many E-Mail security functions is called Ironport.

Ironport provides several E-Mail solutions for corporate environments. One of these products is their PXE architecture. PXE uses PKI Public Key Infrastructure to provide encryption protection for sensitive messages arriving and leaving an organization. It can provide compliance for HIPAA, SOX, GLB and other industry regulations. This is accomplished by sending all E-Mails to be evaluated by the PXE server. The Ironport server screens these messages for content that is subject to protection, such as medical information, or other sensitive business information. This is done by scanning the message header, body and also attachments. This way the decision can be made on a case by case basis on whether or not a message warrants encryption protection. Messages can even be bounced back to the sender if they are not suitable for

release. If Ironport determines that a message warrants encryption, then the Ironport server works together with the Ironport Key Server to provide keys and signatures to encrypt a message. There is a Hosted Key service that can provide control for these keys, or an organization can provide key services themselves on a server if extra management control is needed. Once the key is obtained the message is encrypted and sent to its destination [2].

Upon delivery the recipient can open the message in any client and see a message for how to obtain the decryption key. They will be directed to the Ironport Hosted Key Server to input their information or create a profile. Once this is done, they are assigned a public/private key pair and given the public key for the sender of the message. The public key is then used to decrypt the secure message. This setup prevents users from having to go to a certificate authority to generate a certificate before receiving encrypted messages [1]. Users can read Ironport encrypted E-Mails through Outlook or any web based E-Mail client as well [2].

Ironport can also provide other E-Mail security functions. Messages can be locked from reading before or after a certain date. This can keep time sensitive information from being exposed early or inaccurate message from propagating when it is no longer valid. Certificates used with Ironport provide a unique identity for E-Mails sent and can also provide guaranteed read receipts. This provides acknowledgement that a message was received and even read. Ironport traditionally focused around spam E-Mail filtering before moving into other areas of the E-Mail market. Their spam filtering is among the best and with proper filter settings can filter most spam out of a user's

inbox. Ironport is a server based setup that can provide answers to many of the common E-Mail security concerns today [2].

Encryption is slowly moving into all forms of E-Mail service as users become savvier and their security needs increase. Even yahoo has announced that they will offer encryption to their webmail users. A planned deal between Yahoo and an encryption company named ZixIt will provide this service. ZixIt's ZixMail reportedly allows messages to be scrambled so they cannot be read in transport from sender to receiver. As E-Mail encryption becomes more popular, there are sure to be more webmail providers to follow suit [6].

Another possible E-Mail encryption technology uses XML to provide end to end encryption for messages. Typical S/MIME and PGP solutions only encrypt the body of the message and not header information. This can still be a security risk since hackers that gain this information can use it to hack or spam the specified addresses. The technology described would produce E-Mails in an XML format allowing the use of security protocols that are already built into XML. Developing a technology such as XML E-Mail could provide many of the services of S/MIME and PGP, but add the ability to encrypt entire messages to protect the message header and body during transport [9].

Despite all the development of message encryption to protect the privacy of messages, there will still be some spam messages or messages that contain malware and viruses being received. This is where anti-virus servers and spam filtering servers come into play. There is a wide array of choices when it comes to E-Mail filtering products. The aforementioned Ironport is one such product that provides these functions. A

product that can scan incoming and outgoing mail for viruses and malware is a must for many organizations to protect their users [2].

Spam filtering is among one of the biggest topics in E-Mail security. Most spam filters today divide E-Mails into two categories, spam and non-spam. Often legitimate messages will be incorrectly placed in the spam folder by a spam filter. When this situation occurs it requires the user to search through all the spam to find that one legitimate message that was incorrectly categorized. A paper by IEE members Zhu and Zhao strives to provide a better solution than placing all spam suspected mail into one folder. In their paper they suggest that E-Mail be divided up further into at least three categories, spam, suspected spam and legitimate mail. A setup like this would make it much easier to find legitimate messages that are incorrectly categorized by the spam filter. Since most spam would go to the spam folder and only a few messages would be sorted into the suspected spam folder making it much easier to find messages that do not get placed directly in the inbox [12]. Although fighting spammers is an ongoing battle, software like this could put security professionals a step ahead of hackers aiming to use E-Mail as their hacking tool.

Authentication

Just as important as protecting E-Mail data as it travels the Internet, is protecting an end user's mailbox access. A large part of controlling this E-Mail access is the authentication process. Authentication methods are a popular topic in the aspect of security in other communications protocols. Many of the same authentication methods can be applied to E-Mail to protect mailbox access for sending and receiving messages.

It is quite common for E-Mail users to have to enter a text password to authenticate themselves to an E-Mail server before access their mailbox. This method is often broken easily as users commonly forget or store passwords in the open. A method of authentication that is used in other security applications is the use of smart cards. These are identification cards that contain a chip or barcode that can be read to identify an individual. The method of reading can be through rfid or swipe. There have been several methods proposed that apply this authentication scheme to E-Mail. This would typically require a card reader be attached to end users computer or E-Mail device. When a user wanted to access their E-Mail account, they would swipe the card and the computer would use the information on the card to authenticate to a database. A PGP key or other digital ID would be placed on the card to identify the user. This information would also be used to encrypt further E-Mail communications between the device and server. Java may be a good platform to design code as many of these functions currently built in to the code base [8].

Another authentication method commonly considered by IT staff is fingerprint authentication. In this scenario, a user would be prompted for a fingerprint scan before accessing E-Mail. In many cases a fingerprint can be read faster than a user can enter a password, so replacing password authentication can speed up the logon process. Fingerprint authentication could be used in the same manner as a smart card to initiate PKI encryption between the E-Mail server and the client. PKI encryption would still require secure storage of keys on a usb key or other media. Fingerprint reader hardware would be necessary to allow this scheme to work, but it is becoming more common for

computers to have this hardware built in from the factory [13]. Several of these factors are making fingerprint authentication an effective method of authentication for E-Mail.

Conclusion

More and more people rely on E-Mail for simple and easy communication every day. In order to take advantage of its strengths, E-Mail processes need to be reviewed and updated as newer protocols and technologies are developed. There is not one good answer for every organization or individual's E-Mail problems. Good solutions take the different options from client, server and authentication methods, then use the technologies and solutions that can be best applied to the particular situation. The most successful E-Mail systems use the best options together to allow users to access E-Mail the easiest and most secure way possible.

References

[1] Anonymous (2008, 2/6). Using Digital Signatures. *2008(3/10,* Available: http://www.entourage.mvps.org/smime/index.html,

[2] Anonymous (2007, IronPort PXE encryption technology: safeguarding business email. *IronPort Whitepaper* Available: http://ironport.market2lead.com/go/ironportinc/WP_PXE_Encryption

[3] Anonymous (2006, 4/26/2006). Multipurpose internet mail extensions. *2008(3/19),* Available: http://www.mhonarc.org/~ehood/MIME/

[4] Anonymous (2000, 3/28/2000). PGP, PGP/MIME, OpenPGP, and S/MIME: A short history. *2008(3/19),* Available: http://www.uic.edu/depts/accc/newsletter/adn26/history.html

[5] J. Beck. Email explained. *2008(3/18),* Available: http://www.sendmail.org/resources/email-explained.php

[6] P. Festa. (2000, 8/25). Yahoo to offer Encrypted Email Option. *CNet News 2008(3/10),*

[7] P. Hoffman. Http://www.imc.org/smime-pgpmime.html. *2008(3/10),*

*[8] G. Kardas, "A Smart Card Mediated Mobile Platform for Secure E-Mail Communication," *Information Technology, 2007. ITNG '07. Fourth International Conference on,* pp. 925-928, 2007.

*[9] L. Liao, "Secure Emails in XML Format Using Web Services," *Web Services, 2007. ECOWS '07. Fifth European Conference on,* pp. 129-136, 2007.

[10] P. Slavic. (2004, 05-01-2004). A Quick Guide to Email Security and What's Wrong with a Generic Antivirus Program. *2008(3/10),*

[11] H. Tschabitscher. (2008, SMTP inside out. *2008(3/18),* pp. 2. Available: http://email.about.com/cs/standards/a/smtp.htm

*[12] Wenqing Zhao, "An Email Classification Scheme Based on Decision-Theoretic Rough Set Theory and Analysis of Email Security," *TENCON 2005 2005 IEEE Region 10,* pp. 1-6, 2005.

[13] Zhe Wu, "A Secure Email System Based on Fingerprint Authentication Scheme," *Intelligence and Security Informatics, 2007 IEEE,* pp. 250-253, 2007.