E-MAIL SECURITY

The electronic mail system (e-mail) is an internet application in which users can exchange messages, links, and attachments (files, photos) based on point-to-point communication; it acts as a quick way to share data between users. Given our growing reliance on electronic mail, there is also an increasing number of attacks, and some other security problems. Therefore, specific protocols are required to provide end-to-end security for e-mail.

The internet mail system includes two subsystems.

The First Subsystem is the message user agent (MUA), which is a software agent, such as Google Gmail, Microsoft Outlook, Yahoo, or Apple Mail, that facilitates end user interaction with web content by acting on behalf of the user to compose, send, reply, display, and delete messages. MUA also restores messages from a remote server using the Internet Message Access Protocol (IMAP) or the Post Office Protocol (POP). MUA can employ a Message Store (MS), which is the location where an electronic mail system stores its data, such as an Outlook personal storage table (.pst). The MS may be located with the MUA or on a remote server.

The Second Subsystem is the message handling system (MHS), which consists of a message submission agent (MSA) and a message transfer agent (MTA). MSA is a program agent that receives electronic mail data from an MUA and cooperates with an MTA in the delivery of the mail; it uses the extended simple mail transfer protocol (ESMTP), which is a protocol extension of the Simple Mail Transfer Protocol (SMTP) standard in which the sender and the receiver can be authenticated and servers can indicate supported extensions. MSA can be used as a separate functional model or integrated with the MUA. MTA is a software application that adds trace data to the message header and is also responsible for transferring and routing email messages from the sender computer to the receiver computer using SMTP.

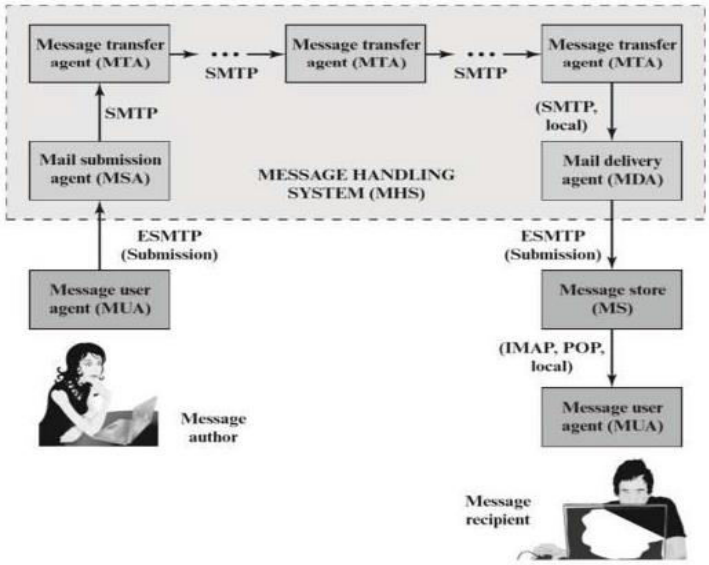

Fig. 1. Process and Key Components of the Internet Mail Architecture [2].

EMAIL SECURITY THREATS AND RISKS

E-mail system exchange messages over networks lack appropriate security safeguard, it is outside the security boundary. Over half of the mails received are spam, phishing campaigns, and malicious, because the core email protocols do not have any mechanism for authentication.

In this electronic world, it is very important for everyone to be aware with the following threats.

- **Eavesdropping:** Type of passive attack, unauthorized access by secretly or stealthily tracking to the private communications or mail messages of others and read them without their consent.

- **Masquerade (Identity Theft):** Type of active attack occurs when someone pretends to be another or different entity. For example, if someone steal your email username and password, then he/she can impersonate your identity without your knowledge and use your account for read and send email messages.

- **Message Modification:** Type of active attack that is stop the flow of the message delay, reorder and optionally modify the message then release the message again to make an unauthorized change. For example, an email meaning "Don't Allow Dalia to Access confidential file accounts" is changed to mean "Allow Dalia to Access confidential file accounts".

- **Repudiation:** Occurs when someone sends an email message and later deny regarding sending of message. For example, emails use as contracts in business or banking communications

- **Unprotected Backups:** All email messages and backups saved in plain text on SMTP server. If someone gets access to these servers, then he can access emails messages even if the origin user deletes them, they can be residing on the severs/backup-servers for years.

- **Email Spoofing:** The creation of email messages with a forged sender address.

- **Email Spamming (junk email):** Unwanted data sent in bulk by email for some malicious intent or for commercial or advertisement purpose, they may include links that drive to phishing web sites or links that are include malware or viruses as attachments file. Spammers gather email addresses from the internet (sites, stock, news, and adult services), these collected email addresses are sometimes also market to other spammers.

- **Email bombing:** Refers to sending big amounts of congruent email to an address to distract the attention from an important email messages or to overflow the mailbox and overwhelm the server where the email address is hosted in a denial-of-service attack.

- **Email frauds:** it is the use of email messages as a means to defraud people for personal, monetary gain or to damage another entity. It can take the form of scam or bargain such as sell popular items at impossibly low prices or investments too good to be true.

- **Emails used as tools to send malicious software:** Some email receive attachments contain destructive viruses, Trojan horses, worms, or spyware, sent intentionally to cause harm, grant network access or steal secret information.

- **Phishing:** The word phishing came from the word fishing, it is the fraudulent attempt to steal your secret information by send an email that appears to be from a legitimate company (banks, IT administrators, social web sites, online payment) which matches the look and feel of the legitimate site and ask you to provide sensitive information such as ATM pin, credit card details, usernames and passwords and use it for any malicious intent.

E-MAIL SECURITY PROTOCOLS

Organization always try to protect the confidentiality and integrity of their electronic mail; therefore, employees do not hesitate to send highly sensitive and confidential information, such as bank reports, and product sales reports, via email. As such, email is the most popular application for exchange this type of information; unfortunately, it is not always secure.

Email messages can be protected using cryptographic methods such as:

1. Signing an email message to verify the identity of its sender and ensure its integrity.
2. Encrypting the email content to ensure its confidentiality.
3. Encrypting the communications between mail servers to protect the confidentiality of both the message body and the header.

The first two method can be done together, although the sender does not always need to encrypt his/her message, such as when the confidentiality of the content does not need to be protected.

When the sender encrypts a message, it is will be signed so that the recipient can guarantee the integrity of the message and verify the signs identity. A copy of each email that travels between servers is always kept on the servers, thus, always encrypt the transmissions between mail servers. In fact, some companies have found a niche in developing specialized software that supposedly erases e-mails from all the servers where they have been archived.

Most encryption methods occur between individual users via email encryption and digitally signing. The most widely used methods to protect e-mail are open pretty good privacy (OpenPGP) and S/MIME. These are protocol-based public-key cryptography methods since the sender and the receiver have a pair of keys: a public and a private key.

PROTECTION AND BEST PRACTICES TO MAINTAIN SECURITY IN EMAIL SYSTEM

A. Filtering Spam Email:

Spam emails are undesirable, unsolicited and un-ratified email messages that dispatched indiscriminately to a group of users. In spam email, the sender's identity is concealed by the spammers, and the receiver does not request the email.

Spam emails lead to annoyed computer users; decrease the work efficiency; increase bandwidth consuming; increase storage space, increase viruses, Trojan horses, worms, and money losses via denial of service and phishing.

Spam email has become an increasing hassle in current years. It has been estimated that around 70% of all emails are spam emails. When an email is sent, it passes several servers until it reaches the recipients mailbox. Therefore, spam filters can be set up at strategic locations on both the client and the server sides.

B. Email Header:

Email header present the path of the email and it show different information about the email like the sender, receiver, message ID, and transmission time details.

Spammers forge email headers in order to conceal their identities and cover the actual origin of the email. Message contents: Spammers usually use specific words in their email messages to confuse or circumvent spam filters; these words are used to differentiate spam messages from others.

The following are typical words/phrases used in spam emails "free, limited offer, click here, act now, risk-free, lose weight, earn money, and get rich". The text of spam messages also overuses exclamation marks and capital letters.

Spammers use obfuscation techniques to avoid spam filters, such as "breaking a word into multiple pieces, embedding special characters, misplaced spaces, purposeful misspelling, Unicode letter transliteration, and HTML redrawing"

Spammers have also started using images to hide spam messages; they embed the spam message in an image and send it as an email attachment. Such spam images may not be detected by filtering programs.

Usually, spam images are generated via discrete modifications to a template image, making signature based detection methods ineffective; furthermore, they are obscured to prevent optical character focus (OCR) equipment from analyzing the embedded text.